Extending Safety Assessment Methods for Remotely Piloted Aircraft Operations in the National Airspace System

by

Alexander C. Horrell

B.S. Systems Engineering
United States Air Force Academy, 2010

SUBMITTED TO THE DEPARTMENT OF AERONAUTICS AND ASTRONAUTICS
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN AERONAUTICS AND ASTRONAUTICS
AT THE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

JUNE 2012

Signature of Author: _____
Department of Aeronautics & Astronautics
May 24, 2012

Certified by: _____
Deborah J. Nightingale
Professor of Aeronautics & Astronautics and Engineering Systems Division
Thesis Supervisor

Certified by: _____
Roland E. Weibel
Technical Staff, Surveillance Systems Group, MIT Lincoln Laboratory
Thesis Supervisor

Certified by: _____
Ricardo Valerdi
Associate Professor of Systems & Industrial Engineering, University of Arizona
Thesis Supervisor

Accepted by: _____
Eytan H. Modiano
Professor of Aeronautics & Astronautics
Chair, Graduate Program Committee

Disclaimer:

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

Extending Safety Assessment Methods for Remotely Piloted Aircraft Operations in the National Airspace System

by

Alexander C. Horrell

Submitted to the Department of Aeronautics and Astronautics on 24 May 2012 in Partial Fulfillment of the Requirements for the Degree of Master of Science in Aeronautics and Astronautics

Abstract

Remotely Piloted Aircraft operations are growing rapidly in the United States specifically for the Department of Defense to achieve training needs. To ensure the safety of the National Airspace System is maintained to a high standard, Remotely Piloted Aircraft operations are being assessed on a case by case basis by the Federal Aviation Administration for approval of a Certificate of Authorization. FAA guidance currently requires the use of human observers to ensure safe separation of RPA operations from other aircraft. The United States Air Force intends to use technology to replace the human observers, but a safety assessment must be conducted for approval of any such technology. The objective of this thesis is to examine the process and results of traditional safety assessment methods used by the United States Air Force as well as apply the same information as a case study to an innovative method called the influence matrix framework. The influence matrix framework will be analyzed by applying a clustering technique to gain insight about the benefits and challenges of the assessment method for future systems.

RPA operations at Cannon Air Force Base, NM propose the use of ground-based radars to monitor the airspace around the RPA. The Air Force Safety Center worked together with MIT Lincoln Laboratory for the safety assessment process of the ground-based radars. The knowledge gained in that process is documented in this thesis. Next, that system architecture is further applied to the influence matrix framework for analysis. The influence matrix represents the expected influence of element behavior changes on hazard risk. The framework is manipulated with a clustering technique to analyze results when changing the scope of the safety assessment method.

In this work, the application of the influence matrix provided insights into the functionality of the ground-based radar system and usefulness of the IM method. The clustering technique provided a foundation for a formal process to handle scoping challenges for future complex system safety assessments. For the future, this research will have to be expanded further to better formalize the modeling and assessment of the influence matrix.

Thesis Supervisor: Deborah J. Nightingale
Title: Professor of Aeronautics & Astronautics and Engineering Systems Division

(this page intentionally left blank)

Acknowledgements

I would like to thank MIT Lincoln Laboratory in its entirety and especially the leadership of Dr. Eric Evans and Col. (ret) John Kuconis, Division 4 Director Dr. Israel Soibelman, and Group 42 Leader Gregory Hogan for supporting my research during my two years here. I would also like to extend my gratitude to the UAS Airspace Access Team under the direction of Dr. Rodney Cole, for the research assistantship opportunity. My experience at Lincoln Laboratory has been thoroughly enjoyable and it will be something I will never forget.

I want to extend my deepest appreciation to Dr. Roland Weibel and Dr. Ricardo Valerdi for their patience and insight as my thesis supervisors throughout my time here at MIT. The feedback you provided me during my research and thesis writing process was timely and very helpful in producing quality work. I am truly grateful that you each invested time in me, even when you both are extremely busy, to ensure I remained focused and on track.

I want to thank Dr. Deborah Nightingale for providing the direction to my research and suggestions for different ways to look at my project. I appreciate the opportunity you gave me to work together with the Lean Advancement Initiative staff even though I spent so much time at Lincoln Lab.

Many thanks go to Tina Huynh and Dr. Kenneth Pascoe at the Air Force Safety Center for working with me to guide my research and provide the information I needed to complete this thesis.

Numerous members of the Group 42 staff helped me learn so much over the past two years, that I could not cram it all in this document. In particular, I would like to thank Thomas Billingsley, Evan Maki, Caroline Fernandes, Dan Griffith, and Andrew Weinert for their technical expertise. I also want to thank my officemates, Matthew Molinario and Eric Harkleroad, for putting up with my life commentary and distractions while working.

I appreciate the constant love and support from my family and especially Laura Bakke over the past two years. The confidence you give me to succeed pushed me every day to work hard and complete this thesis. Your thoughts and actions mean so much to me. I love you all!

Further support from my friends all over this country has been a blessing. Thank you to all of you from back home, the USAF community and my new friends here at MIT. All of you make my life more enjoyable and help shape who I become as I continue my career in the Air Force.

Last but not least, I am grateful to God for the opportunity He has given me to be a part of the MIT community and surrounding me with wonderful people. It has been a "once-in-a-lifetime" experience which I will truly cherish.

(this page intentionally left blank)

Contents

1 Introduction **13**

1.1 Motivation 14

1.1.1 Increasing Remotely Piloted Aircraft Operations 14

1.1.2 Federal Aviation Administration Policy 16

1.1.3 Sense and Avoid 17

1.1.4 Safety Assessment 18

1.2 Approach 18

2 Background **19**

2.1 The National Airspace System 19

2.2 Aircraft Flight Rules 19

2.3 Airspace Classifications 21

2.4 Safety Assessment 23

2.4.1 Functional Hazard Assessment 24

2.4.2 Fault Tree Assessment 26

2.4.3 System Design and Architecture Document 26

2.4.4 Concept of Operations/Employment 27

2.4.5 Risk Management Document 27

2.5 Influence Matrix Framework 28

2.6 Discussion and Summary 28

3 GBSAA System Description **31**

3.1 Cannon AFB Operations 31

3.2 Generic GBSAA System 34

3.3 Cannon AFB GBSAA System Elements 35

3.3.1 Ground Control Station 36

3.3.2 Radar Data Processing 37

3.3.3 Air Traffic Control 38

3.3.4 Remotely Piloted Aircraft 39

3.3.5 All Other Air Traffic 40

4 Safety Assessment Process Application **41**

4.1 Introduction 41

4.2 Safety Assessment Process 41

4.3 Hazard Identification 43

4.4 Scoping the Assessment 44

4.5 Detailed Assessment and Modeling 45

4.5.1 Functional Hazard Assessment Application 45

4.5.2 Fault Tree Analysis Application 46

4.6 Discussion of the Safety Assessment Completed for Air Force 47

5 Influence Matrix Framework **49**

5.1 Influence Matrix Framework Motivation 49

5.2 Influence Matrix Framework Description 50

5.3 Influence Matrix Framework Application 51

5.4 Discussion of Influence Matrix Application 56

6 Clustering Application **59**

6.1 Motivation to Explore Clustering Techniques 59

6.1.1 Dependency Structure Matrix Format 60

6.1.2 Clustering Techniques 61

6.2 Selected Clustering Technique for Influence Matrix 63

6.3 Clustering Technique Application 67

6.3.1 Rearrangement Process 67

6.3.2 Cluster Identification 70

6.4 Discussion of Clustering Results 73

6.5 Summary of Clustering Application 88

7 Conclusions and Future Research **91**

Appendix A **95**

Appendix B **97**

Appendix C **101**

Appendix D **105**

Bibliography **115**

List of Figures

Figure 1: Worldwide DoD RPA Operations 15
Figure 2: DoD RPA Base Locations 15
Figure 3: Example Sensing Architecture 17
Figure 4: Airspace Classifications 22
Figure 5: Hazard Risk Index Matrix 25
Figure 6: Cannon AFB Local Airspace 32
Figure 7: Diagram of GBSAA System 33
Figure 8: Example GBSAA System Diagram 34
Figure 9: GBSAA Architecture Diagram 35
Figure 10: Aircraft Control Console built by General Atomics 36
Figure 11: Safety Assessment Process Diagram 42
Figure 12: Example Influence Matrix 50
Figure 13: Definition of Influence 50
Figure 14: Influence Matrix Framework 53
Figure 15: Dependency Structure Matrix 61
Figure 16: Influence Matrix separated by Major System Groups 66
Figure 17: Rearrangement Shapes 68
Figure 18: First Cluster with Pilot as Central Element 71
Figure 19: Second Cluster with Pilot as Central Element 71
Figure 20: Fourth Cluster with Pilot as Central Element 72
Figure 21: Clusters with Pilot as Central Element 75
Figure 22: Clusters with RPA as Central Element 76
Figure 23: Clusters with Radar as Central Element 77
Figure 24: Cluster Comparison 79
Figure 25: Venn Diagram for Cluster Comparison 80
Figure 26: Hazard Comparison by Category 84
Figure 27: Three Example Clusters 85
Figure 28: Large Example Cluster 87

(this page intentionally left blank)

Acronyms and Abbreviations

AFB	Air Force Base
AIM	Aeronautical Information Manual
ATC	Air Traffic Control or Controller
ATM	Air Traffic Management
CFR	Code of Federal Regulation
COA	Certificate of Authorization
CONEMP	Concept of Employment
CONOPS	Concept of Operations
CONUS	Continental or Contiguous United States
DAU	Defense Acquisitions University
DHS	Department of Homeland Security
DoD	Department of Defense
DOT	Department of Transportation
DSM	Dependency Structure Matrix
EO	Electro Optical
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
GBSAA	Ground-Based Sense and Avoid
GCS	Ground Control Station
GPS	Global Positioning System
IFR	Instrument Flight Rules
IMC	Instrument Meteorological Conditions
LOS	Line of Sight
MAC	Mid-Air Collision
MOA	Military Operating Area
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NMAC	Near Mid-Air Collision
NOAA	National Oceanographic & Atmospheric Administration

PIC	Pilot in Command
PIO	Pilot Induced Oscillation
RAPCON	Radar Approach Control
RF	Radio Frequency
RMD	Risk Management Document
RPA	Remotely Piloted Aircraft
SAA	Sense and Avoid
SATCOM	Satellite Communication
SO	Sensor Operator
SSH	System Safety Handbook
UA	Unmanned Aircraft
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
USAF	United States Air Force
VFR	Visual Flight Rules
VHF	Very High Frequency
VMC	Visual Meteorological Conditions
ZCA	Zero Conflict Airspace

Chapter 1

Introduction

The United States Department of Defense (DoD) is increasing the use of Remotely Piloted Aircraft (RPA) in military operations. The rapid increase of worldwide RPA operations over the last ten years has led the Department of Defense to increase RPA operations within the National Airspace System (NAS) to meet training needs. The Federal Aviation Administration (FAA) publishes guidance requiring human observers located in a chase aircraft or on the ground along the flight path to monitor the airspace to ensure the RPA is safely separated from other aircraft [1]. The use of human observers is limited in flexibility and has a high cost. Therefore, the use of Ground-Based Sense and Avoid (GBSAA) technology is being proposed for use to ensure safe separation [2]. The GBSAA architecture utilizes ground-based radar to provide surveillance of local air traffic, allowing an RPA operator to avoid intruders.

For technology to be used, the FAA requires a Certificate of Authorization (COA). Applying for a COA requires a safety assessment and review process before the concept is approved for operation [1].

For a safety assessment, there is no one specific required method. Many different methods are available [3]. Often methods are used in combination to assess the safety of a proposed operation or system. Traditional assessment methods will be applied to proposed RPA operations at Cannon Air Force Base, NM as a part of a Risk Management Document (RMD).

Participation in the generation of the RMD will serve as the basis for this thesis. The objectives of this thesis are to (1) discuss the research and results of traditional methods used by the United States Air Force Safety Center, (2) use the same RPA operation information as an individual case study application for the influence matrix framework. The influence matrix (IM) framework models the system in a matrix format and describes the level of influence the particular system elements have on a given

hazard. This thesis will extend the use of the influence matrix framework by applying it to an additional case study and analyze the insights gained.

First, background is provided on the current National Airspace System and how RPA operations can be integrated. Second, the motivation for assessing the safety of those operations will be explained followed by providing definitions and discussion for various specific safety assessment methods. In Chapter 3, the system architecture for the specific RPA operation at Cannon AFB will be defined and explained. This architecture will be used to assess the safety of the system using traditional assessment methods and the IM. In Chapter 4, the research conducted with the Air Force Safety Center will be explained through the application of traditional safety assessment methods. Following that, Chapter 5 will apply the same RPA architecture to the IM as a separate case study for this thesis. Chapter 6 will assess the use of clustering techniques to manipulate the IM to gain insights about the framework and the overall system safety assessment.

1.1 Motivation

1.1.1 Increasing Remotely Piloted Aircraft Operations

In recent years, the United States has increased RPA operations because of DoD military operations. The increasing number of flight hours for RPAs in shown in Figure 1. As of 2009, RPAs flew approximately 500,000 flight hours in Operation Enduring Freedom and Operation Iraqi Freedom [4]. As of June 2011, the U.S. Government managed more than 6,000 remotely piloted aircraft across the various branches: Army, Air Force, Navy, Marines, and Coast Guard [5]. The high volume of operations and number of RPA managed by the United States requires testing, training, and support operations within our borders to improve the operations and equipment used around the world.

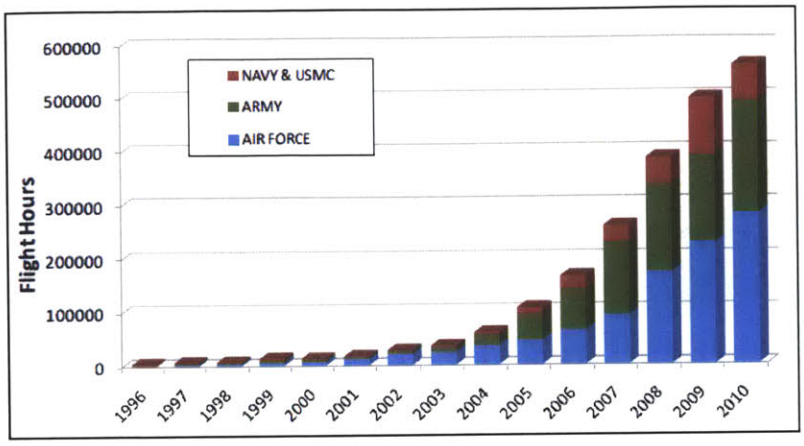


Figure 1: Worldwide DoD RPA Operations [6]

As explained in the Unmanned Aircraft System Airspace Integration Plan, the DoD currently has 146 RPA units based at 63 contiguous United States (CONUS) locations. By 2015, the Joint UAS Center of Excellence (JUAS COE) estimates the DoD will have 197 units at 105 locations - a 35% increase in units and 67% increase in number of locations [6]. Figure 2 shows the expansion of DoD RPA base locations in the United States. With this planned rapid expansion, there is a clear need for more RPA to operate within the same airspace as civilian traffic, and because most planned basing locations are not underneath restricted airspace. It is expected that the FAA will have to review more safety assessments built for a COA, or an approved technical solution may be implemented.

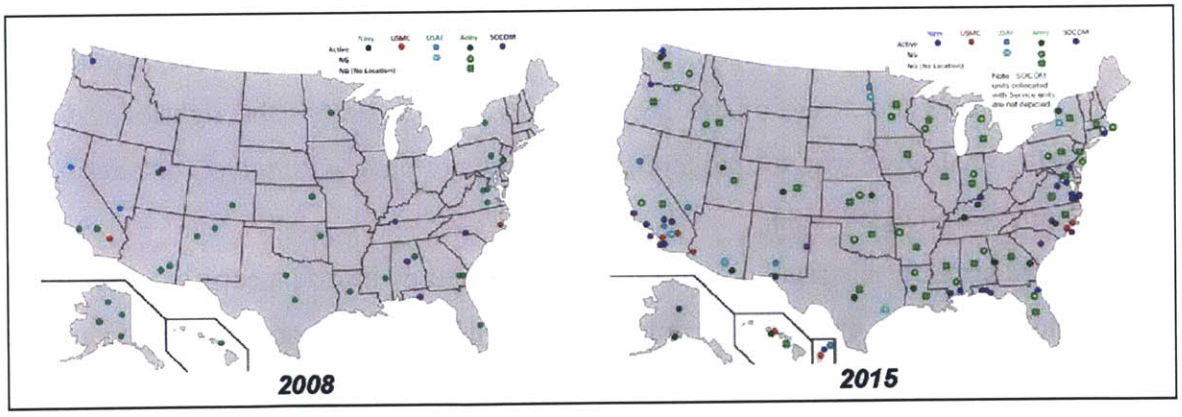


Figure 2: DoD RPA Base Locations [6]

The DoD is not the only entity that has a desire to increase RPA operations in the National Airspace System. The Department of Homeland Security indentified a need for a more constant surveillance capability since manned vehicles are limited by the operator.

The National Oceanographic & Atmospheric Administration (NOAA) proved to the United States that RPA surveillance can be very useful for storm surveillance where situations would be too risky for human pilots [7]. A NASA RPA monitored a 40,000 acre forest fire from a high altitude for over 16 hours as well as provided surveillance for sea lions and seals from a safe distance along the California coast [8]. The U.S. Coast Guard developed a RPA helicopter for future search and rescue missions. The City of Tucson in Arizona uses a RPA helicopter to spray wetlands for mosquito control and has been doing so for more than five years [7]. In June 2011, North Dakota police officers solicited the use of a RPA to help find and monitor armed suspects in a large open area [9]. These examples reinforce the need to safely integrate RPAs into the NAS for more than just military operations.

1.1.2 Federal Aviation Administration Policy

The FAA provides specific policies to dictate requirements for the integration of RPAs within the National Airspace System (NAS). The FAA is primarily concerned with the safety of all the users of the NAS and regulations are established to promote a safe environment for all military and civilian users [10]. Federal Aviation Regulation (FAR) 14 CFR Part 91.113 (b) states:

> "When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft. When a rule of this section gives another aircraft the right-of-way, the pilot shall give way to that aircraft and may not pass over, under, or ahead of it unless well clear" [11].

For manned aircraft, this regulation is currently satisfied by having a certified pilot in the cockpit to monitor the environment directly around the aircraft. Remotely piloted aircraft do not have pilot aboard the vehicle. Therefore, technology must be used to allow the operator to function in the same capacity from the ground.

The challenge for RPA to "see" other aircraft drives special policies and safety analysis to determine if the RPA is safe enough to fly in the NAS. Current FAA regulations permit RPA operations within special use airspace where other aircraft will

not interfere, but to operate outside those special areas the FAA requires a "Special Airworthiness Certificate – Experimental Category" or "Certificate of Waiver or Authorization" [10]. To obtain either, each operation must undergo a review by the FAA to determine if the operation is safe.

The proponent RPA operations that seek a Certificate of Authorization (COA) or Special Airworthiness Certificate must provide a solution in lieu of human visual observers that has been determined safe by the FAA. Each safe solution must show how the RPA can "see" and "avoid" other aircraft. The function of seeing other aircraft can also be performed by sensors such as radar. The technology solution will be referred to as "sense" rather than "see" other aircraft. The use of technology instead of humans must be evaluated and tested for the FAA to determine if the system is safe to satisfy Regulation 14 CFR Part 91.113.

1.1.3 Sense and Avoid

A RPA operator cannot act as a typical pilot onboard the aircraft by simply using his senses to monitor the environment. Therefore, procedures applied to RPA operations differ. Since a remotely piloted aircraft does not have a pilot physically located in the aircraft to "see" the surrounding environment, the operator of the RPA must rely on the capabilities of various sensors and the communication of those results to the operator.

Figure 3 shows the basic systems needed for RPA sense and avoid. The "sense" capability stems from the system function to detect and track other aircraft. The "avoid" capability comes with the performance functions of the aircraft to maneuver in such a manner that a collision does not occur [12]. For remotely piloted aircraft, systems must work together to perform the "sense and avoid" functions. Air traffic in the airspace must be detected by a sensor and that data will then be processed through algorithms to transfer that data into a readable format on the airspace display for the human operator.

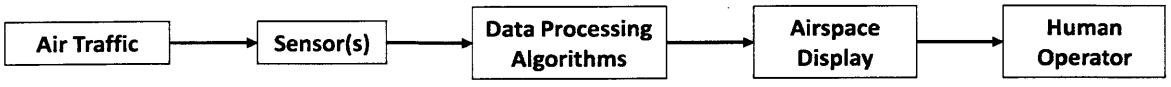


Figure 3: Example Sensing Architecture

For context, the rest of this thesis describes the assessment of using ground-based sensors and displays to enable an operator within a control station to sense and avoid. A

so called Ground-Based Sense and Avoid (GBSAA) system allows the RPA to operate within a determined coverage volume where a ground-based sensor can detect and track any aircraft in the area. The RPA operation at Cannon AFB provides a detailed example of the GBSAA system and is explained in Chapter 3.

1.1.4 Safety Assessment

In order to have the FAA approve a COA, specific policies and guidelines must be followed by an applicant organization [13]. The applicant organization for the case study in this thesis is the United States Air Force. The USAF is seeking a COA for GBSAA in lieu of visual observers. The application stems from FAA policy guidance, stating:

> "Applicants proposing 'see and avoid' strategies in lieu of [human] visual observers, need to support proposed mitigations with system safety studies which indicate the operations can be conducted safely. Acceptable system safety studies must include a hazard analysis, risk assessment, and other appropriate documentation that support an 'extremely improbable' determination" [1].

This guidance requires the USAF, in seeking a COA, to perform a safety assessment. This thesis will explore the safety assessment process, specifically the tools and methods used to conduct hazard analysis and scoping strategies as they are applied in the case study.

1.2 Approach

The approach of this thesis is to gather data in collaboration with the Air Force Safety Center using traditional safety assessment methods. Then, the data gathered is then applied as a case study to extend the influence matrix framework. The IM describes the relationship between system elements and hazards by coupling them together based on the influence each element has on that particular hazard. It is expected to provide the assessor insights about the specific GBSAA functionality and describe safety behavior. The results and insights gained are compared to the traditional methods used and their impact on safety assessment methods for future systems.

Chapter 2

Background

This chapter will provide the necessary background information for the reader to better understand the proposed RPA operations at Cannon AFB. This chapter is organized by first providing a brief description of the NAS, aircraft flight rules, airspace classifications, and specific safety assessment tools and methods used by the Air Force Safety Center applied to Ground-Based Sense and Avoid (GBSAA).

2.1 The National Airspace System

The Federal Aviation Administration (FAA) is the United States agency within the Department of Transportation (DOT) that is responsible for the regulation and oversight of civil aviation. The FAA maintains the operation and development of the NAS that includes air navigation facilities, equipment, services, airports or landing areas, aeronautical charts, information, services, rules, regulations, procedures, technical information, manpower, and material [14]. Even some military systems are included as they interact within the NAS.

2.2 Aircraft Flight Rules

The distinction between different flight rules is relevant to the GBSAA system because they dictate what type of aircraft and safety equipment the RPA operations will encounter in the NAS. When encountering aircraft operating under specific flight rules, the GBSAA system sensor must satisfy requirements to promote a safe environment for the RPA.

There are two sets of flight rules for operating aircraft in the NAS with corresponding weather conditions: visual flight rules (VFR), and instrument flight rules (IFR). Each set of flight rules requires different specific procedures for airspace navigation and interaction with other traffic. IFR flight plans may be required for certain

airspace classifications or types of aircraft operations. Specific weather conditions may also force the aircraft into a specific type of flight rules [15].

Weather conditions are determined by a set of regulations established by the FAA. For visual meteorological conditions (VMC), there is sufficient visibility for the pilot to fly the aircraft based on the use of outside visual cues. Visual meteorological conditions assume the pilot has the ability to see and avoid other aircraft without the assistance of air traffic control (ATC) in most cases. In these conditions, aircraft can fly under visual flight rules. For instrument meteorological conditions (IMC), aircraft instrumentation for navigation is required to enable procedural separation from other traffic as well as communicate and respond to ATC. These conditions require the aircraft to fly under instrument flight rules. Pilots must receive additional training and certification to fly in IMC conditions and the aircraft itself must be equipped with additional instrumentation [15].

For RPA operations at Cannon AFB, there are two types of aircraft the RPA may encounter: non-cooperative and cooperative. Non-cooperative aircraft are those that do not have an electronic means of identification (i.e., a transponder) aboard. Non-cooperative also denotes aircraft where equipment is or not operating due to malfunction or deliberate action. Cooperative aircraft are those that have an electronic means of identification aboard and operating [1].

The electronic transponder is important for aircraft because of the difference between primary and secondary radar systems used in the NAS. The primary surveillance radar system operates independent of the aircraft and does not require a beacon return. The radar sends out energy and the energy reflected off any airborne object is sent back to radar. The primary surveillance radar system requires large amount of energy and when objects are further away, the returned energy may be too weak to provide an accurate location reading. Primary radar returns may even be affected by weather [16].

Secondary surveillance radar uses the electronic transponder to interrogate an aircraft for information. A signal is sent to the aircraft asking it to identify itself. Then, the transponder sends identifying information and altitude back to the receiving station. The signal from the transponder is much stronger than the returned energy from the

primary radar and the transponder provides more accurate position information to air traffic control than the primary radar [16].

The FAA published 14 CFR Part 91.215 stating an aircraft must be equipped with a transponder to fly under IFR because of the higher degree of accuracy associated in altitude provided by the transponder [11]. The accurate altitude information allows air traffic control to ensure safe separation from other aircraft operating in the same area.

The GBSAA system must be able to account for worst case scenario which is VFR aircraft operating between airports without the supervision of air traffic control. This is the worst situation because the VFR aircraft is only relying upon the vision of the certified pilot to see and avoid the small RPA while the RPA is limited by its sensors to see and avoid the VFR aircraft. Adequate sensors must be in place for the RPA to avoid a collision with all aircraft, but if the RPA can avoid the worst case situation, it should be able to avoid all aircraft especially with the help of air traffic control for aircraft operating under IFR.

2.3 Airspace Classifications

The description of airspace classifications is relevant to GBSAA to understand the environment and different procedures the RPA will be operating in local to Cannon AFB. Airspace classifications regulate what type of aircraft and safety equipment the RPA will or will not encounter in each class. When encountering aircraft operating in specific airspaces, the GBSAA system sensor must satisfy requirements to promote a safe environment for the RPA.

As defined by the FAA, the NAS is divided into two area categories: regulatory and unregulatory [15]. Regulatory areas include Class A, B, C, D, E and G airspace as well as restricted and prohibited areas. Unregulatory areas include military operations areas (MOA), warning areas, alert areas, and controlled firing areas [15]. Within these two categories are four types of airspace: controlled, uncontrolled, special use, and other [15]. The operating rules for each airspace classification are different and each operation within those classifications must be assessed differently. They directly impact the COA and safety assessment process for each proposed RPA operation within the NAS. Only a few of these airspace classifications are going to be simply defined because they are

relevant to the proposed GBSAA system operations at Cannon AFB. The detailed explanation of each of these classifications located near Cannon AFB will be explained in Chapter 3.

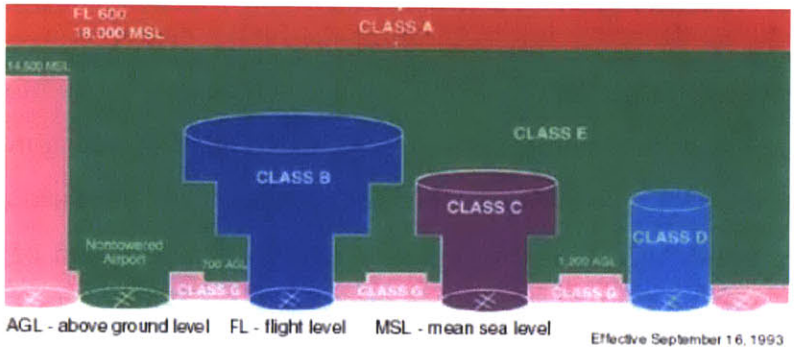


Figure 4: Airspace Classifications [17]

Figure 4 illustrates Class A, B, C, D, E and G airspace. These airspace classifications make up the civil airspace within the NAS. The hierarchy of these classifications is as follows: Class A airspace is more restrictive than Class B; Class B is more restrictive than C; and so on. Class G airspace is the least restrictive out of the six classes. Class G airspace is also the only class of the six that is uncontrolled by FAA services [15].

As defined by the FAA AIM, there are two types of special use airspace are the designation for specific airspace operations:

1) Restricted areas contain airspace identified by an area on the surface of the earth within which the flight of IFR or VFR aircraft, while not wholly prohibited, is subject to restrictions. Activities within these areas must be confined because of their nature or limitations imposed upon aircraft operations that are not a part of those activities or both. Restricted areas denote the existence of unusual, often invisible, hazards to aircraft such as artillery firing, aerial gunnery, or guided missiles. Penetration of restricted areas without authorization from the using or controlling agency may be extremely hazardous to the aircraft and its occupants [15].

2) Military Operations Areas (MOAs) consist of airspace with defined vertical and lateral limits established for the purpose of separating certain military training activities from IFR traffic. Whenever a MOA is being used, IFR aircraft that are not a part of the planned activities and/or airspace activity may be cleared through an MOA if IFR

separation can be provided by air traffic control authorities. Otherwise, the IFR aircraft will be rerouted or restricted from entering. VFR aircraft will exercise extreme caution while flying within a MOA when military activity is being conducted. The activity status of MOAs may change frequently. Therefore, VFR aircraft are advised to contact the local controlling agency for traffic advisories prior to entering a MOA [15].

Restricted airspace and MOAs are illustrated on sectional, terminal area, and enroute charts for use at a particular altitude. These charts are a part of the information governed within the NAS [15]. RPA operations in restricted airspace do not require special authorization by the FAA.

2.4 Safety Assessment

Safety assessment is the structured process of examining safety-related behavior of a system by defining potential hazardous states, determining if hazards meet defined acceptable criteria, and mitigating any deficiencies that do not satisfy that criteria. The assessment process can be performed for a system which is conceptual or already in operation. The techniques and methods used to examine the safety performance of the system are not always the same. Typically, the criteria for acceptable safety performance are defined before the examination is conducted.

Acceptable criteria can be in the form of a required procedure, level of risk, or a measure of system performance [18]. For this thesis, the level of risk is defined as the probability and severity of an accident or loss from exposure to various hazards, including injury to people and loss of resources [3].

Once the system safety performance is evaluated, the results will determine what, if any, action should take place. If the results show the system meets or exceeds the acceptable criteria, then no action may be necessary. If the results show the system does not meet the acceptable criteria of safety, there will need to be mitigation. Mitigation addresses unacceptable levels of risk by defining requirements for a system or changes to the system that will change the performance of the system to meet the acceptable criteria.

The safety assessment process for the RPA operations at Cannon AFB includes several methods and supporting documents to provide a complete evaluation. Remotely Piloted Aircraft are complex systems operating within a complex environment of manned

aircraft. FAA guidance does not define a determined safety requirement, nor does it define what methods or supporting documents should be used to conduct system safety studies. Further detailed guidance for constructing a safety assessment can be found within the SAE ARP 4761 [19], the FAA System Safety Handbook [3], and Military Standard 882E [20].

Currently Cannon AFB is applying for a COA for their proposed GBSAA system. As a part of the COA, Cannon AFB is working together with the Air Force Safety Center in the safety assessment process to present their results to the FAA. The safety center chose a specific set of traditional assessment methods and supporting documents that need to be completed. The first objective of this thesis is to discuss the research and results of those methods. The method results will also be used to build the Risk Management document that will be presented to the FAA as a part of the COA application.

The selected methods and documents are: Functional Hazard Assessment, Fault Tree Analysis, System Architecture Document, and Concept of Employment. Each of these specific methods and documents will be briefly explained through various sources. Each defining source may have slightly different definitions, but the general background knowledge of each will be helpful to understand for this thesis. Each method or document differs in scope and their advantages and disadvantages as they are applied to the safety assessment process. The traditional methods will be applied in a case study for Cannon AFB and will be presented and discussed in Chapter 4.

2.4.1 Functional Hazard Assessment

A functional hazard assessment (FHA) is a method of assessment that can be used to provide inputs to manage risk, expose critical safety failure modes, or assist in operational planning. The FHA can be a qualitative or quantitative analysis. The FHA requires a detailed investigation of the subsystems to determine system components, their hazard modes, causes of these hazards, and resultant effects to the system and its operation. To conduct a fault hazard analysis, it is necessary to know and understand the system elements, operational constraints, success limits, failure limits, failure modes, and a measure of their probability of occurrence. Functional diagrams for the system and each

subsystem are then reviewed to determine their component functionality. Risk levels are assigned to the failures of each system element regardless of whether or not the failure creates a hazard [3].

An FHA analyzes the potential consequences on safety resulting from the loss or degradation of system functions. Using service experience, engineering and operational judgment, the severity and likelihood of each hazard effect is determined qualitatively and is placed in a class. For severity, class 1 refers to the most severe effect and class 5 refers to no effect. For likelihood, class A refers to a frequent occurrence and class E refers to extremely improbable. The acceptable safety criteria determine the maximum tolerable probability of occurrence of a hazard, in order to achieve a tolerable risk level [21]. Figure 5 shows the Hazard Risk Index Matrix and how the likelihood and severity of each hazard can typically be classified as a high, medium, or low risk hazard.

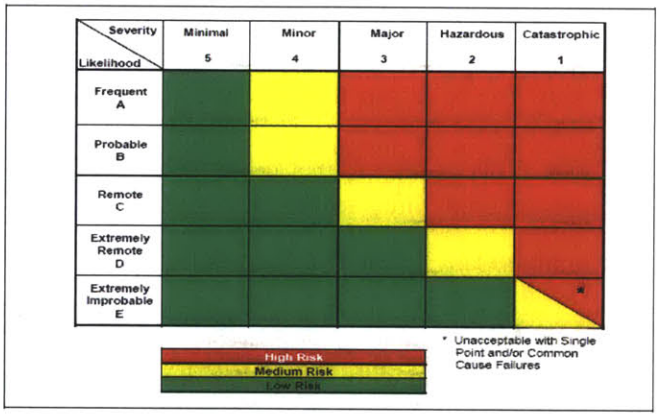


Figure 5: Hazard Risk Index Matrix [22]

For the FHA, the system is evaluated in a functional perspective. This perspective focuses on what rather than how the system produces a desired result. Functions include required receiving inputs, sending outputs, and operating transition tasks. When those functions are lost or degraded, the system will operate differently state, and that can be hazardous to either itself or the environment. The functional perspective provides the assessment an understanding of what systems are critical for safe operation. If a particular system can be prevented from losing its function within the architecture, a hazard may possibly be prevented.

2.4.2 Fault Tree Assessment

A fault tree assessment (FTA) is a method of assessment that has the purpose of finding hazards that result from single-fault events in a system element that may arise from any system mode such as storage, transportation, or operation. It considers the effects of a single fault within a system element and across system interfaces. Since it traces the effects of a single-fault or component failure, it is sometimes called a single-thread analysis [21].

This method is used to both prevent and resolve hazards and failures. It can be used as a qualitative or quantitative method to identify areas in systems that are most critical to safe operation. The FTA is a graphical presentation of a map of failure or hazard paths. It usually begins with a defined undesired event, hazardous condition, and systematically considers all known events, faults, and occurrences that could cause or contribute to the occurrence of the undesired event. Analysis can provide insights into system behavior, particularly the behavior that might lead to a specific hazard [3].

This graphical presentation of the system must include all combinations of system fault events that can cause or contribute to the undesired event. Each contributing fault event should be further analyzed to determine the relationships of underlying fault events that may cause them. This tree of fault events is expanded until all input fault events are defined to a basic level desired by the user. When the tree has been completed, it becomes a logic gate network of fault paths, both singular and multiple, containing combinations of events and conditions that include primary, secondary, and upstream inputs that may influence or determine the hazardous condition [3].

2.4.3 System Design and Architecture Document

A system architecture description is a formal description and representation of a system. The document is organized in a way that supports reasoning about the structure of the system components or elements, the externally visible properties of those elements, and the relationships between them. The system design description provides a plan from which products can be procured, systems developed, and that will work together to implement the overall system [23].

2.4.4 Concept of Operations/Employment

The concept of operations/employment (CONOPS or CONEMP) is a verbal or graphic statement, in broad outline, of a military commander's assumptions or intent in regard to an operation or series of operations. This concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose [24].

For Cannon AFB, the concept of employment describes the proposed GBSAA operations. The selected parts of the CONEMP that will be included in the Risk Management document are: a description of the arrival and departure area, the operational airspace, what systems will be used, possible operating scenarios, and assumptions and risks [2].

2.4.5 Risk Management Document

The safety assessment methods (FHA, FTA, Architecture Description, and CONEMP) will be included within the Risk Management Document (RMD) that Air Force Safety Center is building for the FAA COA application process. The methods used are well established. Several engineering programs and projects have applied these methods over the past decades and can provide many examples [25]. Being even more specific, the FAA outlines the FHA and FTA in their published System Safety Handbook that is used as a guideline for all FAA safety assessment material.

Risk Management is a decision-making process to systematically help identify risks and benefits and determine the best courses of action for any given situation. The risk management process does not wait for an accident to happen, it figures out how to prevent it from happening at all. Risk must be managed whenever a system is modified just as Cannon AFB will be through the use of GBSAA. All FAA operations in the United States require decisions that include risk assessment and risk management [3].

The RMD includes a comprehensive evaluation of the safety risks being assumed prior to operation of the system. It identifies all mitigations for hazards through specific procedural controls and precautions that should be followed [3].

The document collects arguments, evidence and assurance through the assessment methods to ensure that each system element as implemented meets its safety requirements

and that the system as implemented meets its safety objectives throughout its lifetime. It demonstrates that all risks have been identified and eliminated or minimized as far as reasonably possible. This is important for a system to acceptable, so those risks must be monitored for as long as the system is in service [21].

2.5 Influence Matrix Framework

The second objective of this thesis is to apply the influence matrix (IM) framework to GBSAA. The IM framework is an innovative method for describing system safety behavior that uses a matrix format presentation of how system elements influence and relate to hazards [18]. The ability to model connections between system elements and hazards can provide focus areas for risk analysis, mitigation, and test planning because those relationships could highlight important patterns in the architecture.

The IM models the magnitudes of influence in the form of an m x n influence matrix. The "m" columns of the matrix list the system elements, and the "n" rows of the matrix contain the list of identified hazards. Each cell of the matrix is the influence of the corresponding element to that hazard. The level of influence is defined by the matrix author with the use of justification based on data collected and other safety assessment tools [18]. The method will be applied to the RPA operations at Cannon AFB and later explained in Chapter 4.

2.6 Discussion and Summary

The motivation for expanding research through application of the IM is due to some weaknesses and complexity uncovered in the application of the traditional methods described above.

One weakness of the FHA is that it does not discover hazards caused by multiple faults. The FHA is primarily an evaluation of the effects of subsystem component failures in all modes of system and subsystem operating. The FHA draws a clear connection between a system element and its functions, but it does not provide a clear connection to hazards. The FHA may even identify system element failures that may not result in a

hazardous condition. Under some circumstances this can be an inefficient use of recourses.

A weakness of the FTA is that it is a rigid diagram with limited possibilities of describing the system accurately. As the system decomposes into lower levels of detail, multiple system elements may contribute to hazards that are unrelated. It is visually difficult to see just one level of the FTA and understand the hazard that each system element is contributing to. The FTA requires the user to follow the tree from the top to the bottom to better understand each branch as a flow of events or faults. The rigid diagram structure of using an "and" or "or" statement with each branch limits the possibility of how the system is described. A system element may create a hazard with a combination of other elements, but it could create a hazard by itself too. A system element may even behave differently in different conditions that changes it from an "and" to an "or" contribution. Since the FTA is single-fault failure approach that expands downward from that failure, the FTA may miss some non-obvious high level hazard than may not contribute to that specific failure.

Both methods have common weaknesses. It is unclear when to stop applying both methods as more system components can continually be added. An FTA can continually be decomposed further into system elements and hazard faults. This can create a method that has far too many pieces to see on a page or understand quickly. An FHA has a similar problem with not knowing where to stop to have an adequate method.

Another common weakness in the FTA and FHA methods is over precision in mathematical analysis when chosen to provide quantitative results. Analysts try to obtain exact numbers from inexact or expert provided data. Too much time may be spent on improving preciseness of the analysis rather than eliminating the hazards [3].

The influence matrix framework was first constructed in 2009 and will be expanded upon through application with the USAF. The basic motivation for this research is to use the IM to provide a better visual method for the user to understand and model a particular system. The objective of the IM is to show the relationship between system elements and hazards in one clear diagram. The FHA and FTA use multiple steps and large tables full of information to show similar information depicted in a single IM.

The IM application in Chapter 6 expands upon these ideas to gain additional insight about safety behavior than provided by traditional methods.

Chapter 3

GBSAA System Description

In order to apply the safety assessment methods described in Chapter 2 as a case study to the Cannon AFB RPA operations, the proposed GBSAA system must be described. The United States Air Force is seeking a Certificate of Authorization from the FAA to fly RPA training missions through the NAS without human observers to access nearby restricted airspace. This chapter provides details on Cannon AFB RPA operations followed by a detailed description of the GBSAA system architecture.

3.1 Cannon AFB Operations

Cannon AFB is located in Clovis, NM, and is an established training base for RPA equipment and crews because of its close location to restricted airspace and a military operating area [6]. Within restricted airspace, RPA operations can take place within them and the threat of colliding with air traffic is eliminated.

The airspace between the Cannon AFB runway and the restricted airspace or MOA is civil airspace where other air traffic can operate freely. To safely operate RPAs from Cannon AFB to the restricted airspace or MOA, the use of the Ground-Based Sense and Avoid (GBSAA) system is being proposed. The GBSAA system will replace human observers located on the ground. It will utilize the capabilities of ground-based radars to detect air traffic to ensure the RPA remains safely separated while maneuvering in the public airspace. The Air Force Safety Center is evaluating the GBSAA system to determine if it is safe for use in the NAS [2].

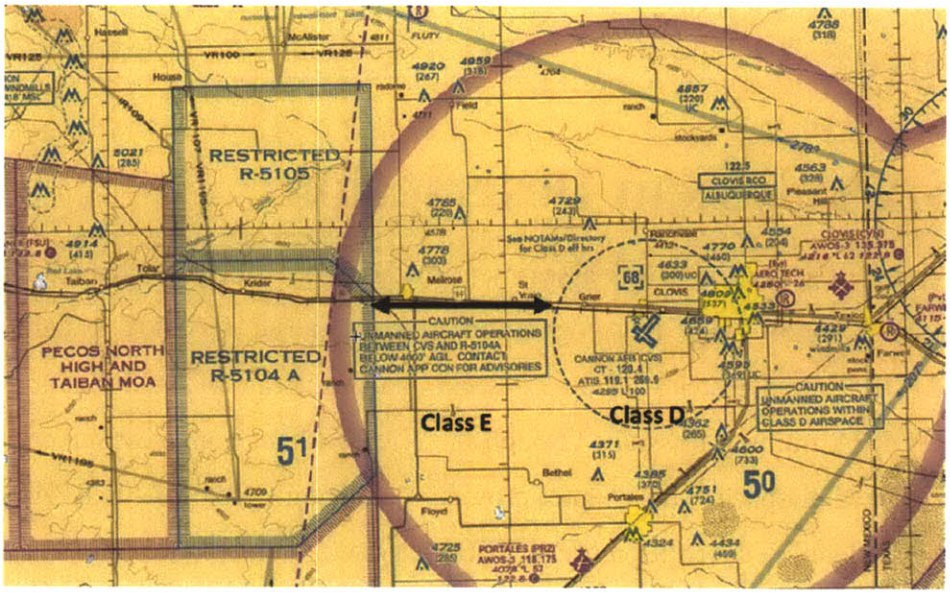


Figure 6: Cannon AFB Local Airspace [26]

Cannon AFB, designated KCVS, is located 5 nm West of Clovis, NM at an airfield elevation of 4,295 feet above sea level [27]. KCVS terminal airspace is shown as a dashed circle around the airfield symbol just to the right of the center of Figure 6. This is Class D airspace from the ground level to 6800 feet and extends out 6 nm in all directions from the airfield. It is controlled by the Cannon AFB Radar Approach Control and any aircraft can be directed how to operate within the airspace [2].

The airspace surrounding the Class D airspace is Class E airspace. It is depicted in Figure 6 by the larger dark circle surrounding the Class D airspace and extends from ground level to 10,000 ft. For the proposed GBSAA plan, aircraft operating in the Class E airspace will be controlled by the Cannon AFB Radar Approach Control [2].

To the left of the Class E airspace in Figure 6 are three boxes that designate restricted airspace and military operating areas. From the outer boundary of the Class D airspace to the outer edge of the restricted airspace is an 11 nm distance represented by the dark arrow in Figure 6 [2].

Class A airspace is positive controlled airspace at and above 18,000 ft. The proposed GBSAA operation specifically prohibits the RPA from entering this airspace. Class B, C, and G airspace are all airspace classifications that are not present around the Cannon AFB RPA operations [2].

Currently, three COAs have been approved by the FAA for RPA operations within Class D airspace and Class E airspace located between Cannon AFB terminal area and the restriced airspace 5104 [2]. The Class E COA requires multiple ground-based observers to monitor the airspace. The Class D COA allows multiple RPAs to operate within the terminal area without extra ground observers because it is controlled and monitored by Cannon AFB Radar Approach Control. The proposed GBSAA system expands upon these exsisting COAs by using technology instead of human ground-based observers and does not alter the existing Class D COA [28].

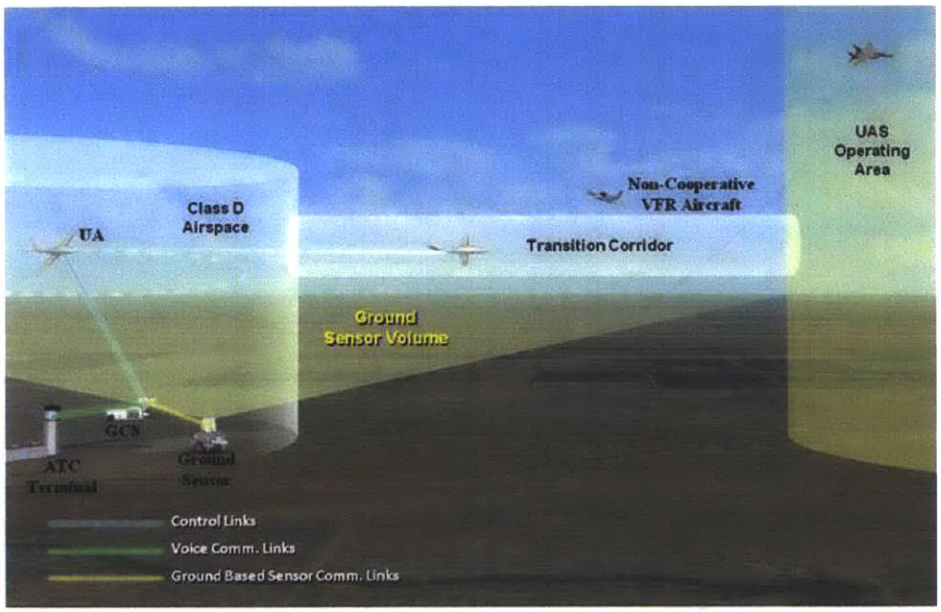


Figure 7: Diagram of GBSAA System [6]

The RPA will depart from the Class D terminal airspace at Cannon AFB and travel to restricted airspace west through a transition corridor shown in Figure 7 and represented by the dark black arrow in Figure 6. Also shown in Figure 7 is the use of ground-based radar(s) to monitor the airspace used for operations.

The airspace the radar will monitor will contain a Zero Conflict Airspace (ZCA). The term "Zero Conflict Airspace" refers to the concept that the RPA crew will ensure a predetermined volume of airspace contains zero non-cooperative aircraft to authorize operations in the Class E airspace. With the ZCA clear, the threat of other aircraft flight paths intersecting with the RPA's will be mitigated allowing for safe transition to the restricted airspace. The RPA crew will even consider any other aircraft that may be

operating closely outside the prescribed ZCA volume to ensure those aircraft are not on course to threaten the RPA. Cooperative aircraft can be allowed in the ZCA if ATC is providing separation services to the aircraft. Cooperative aircraft that are not under ATC control can be considered a threat to the RPA depending upon its flight path [2].

3.2 Generic GBSAA System

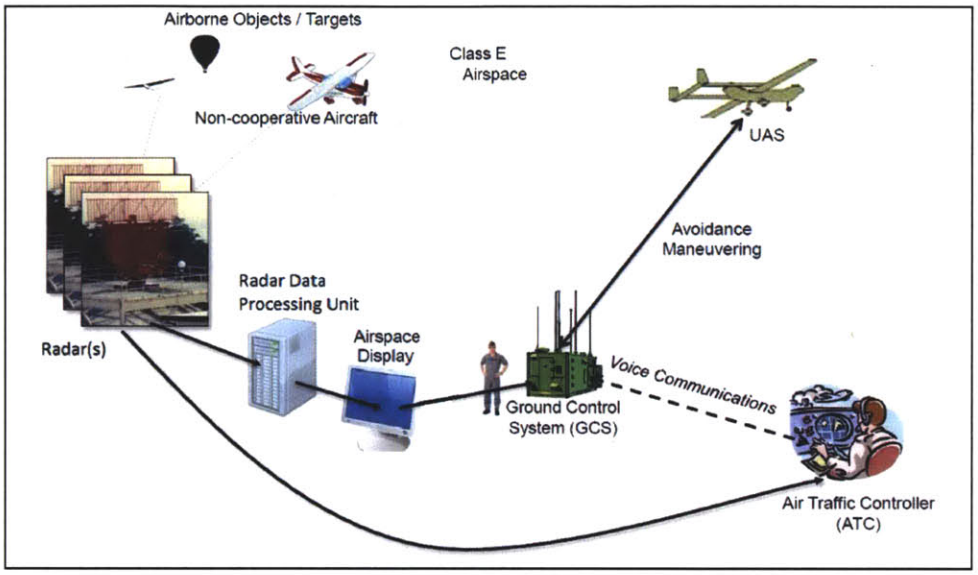


Figure 8: Example GBSAA System Diagram [29]

The basic subsystems necessary to conduct RPA operations using the GBSAA system are shown in Figure 8. The ground-based radar(s) detect aircraft present in the airspace. This same data that Air Traffic Control uses for an airspace display is also sent to a separate data processing unit. The processed data is then sent to an airspace display within the Ground Control Station (GCS) where the RPA operators can visually read the data and be alerted of any unsafe conditions. If a maneuver is needed to avoid a conflict, the operator will execute that maneuver. Voice communications between the GCS and ATC are conducted through Very High Frequency (VHF) radio or via land-line backups [29].

3.3 Cannon AFB GBSAA System Elements

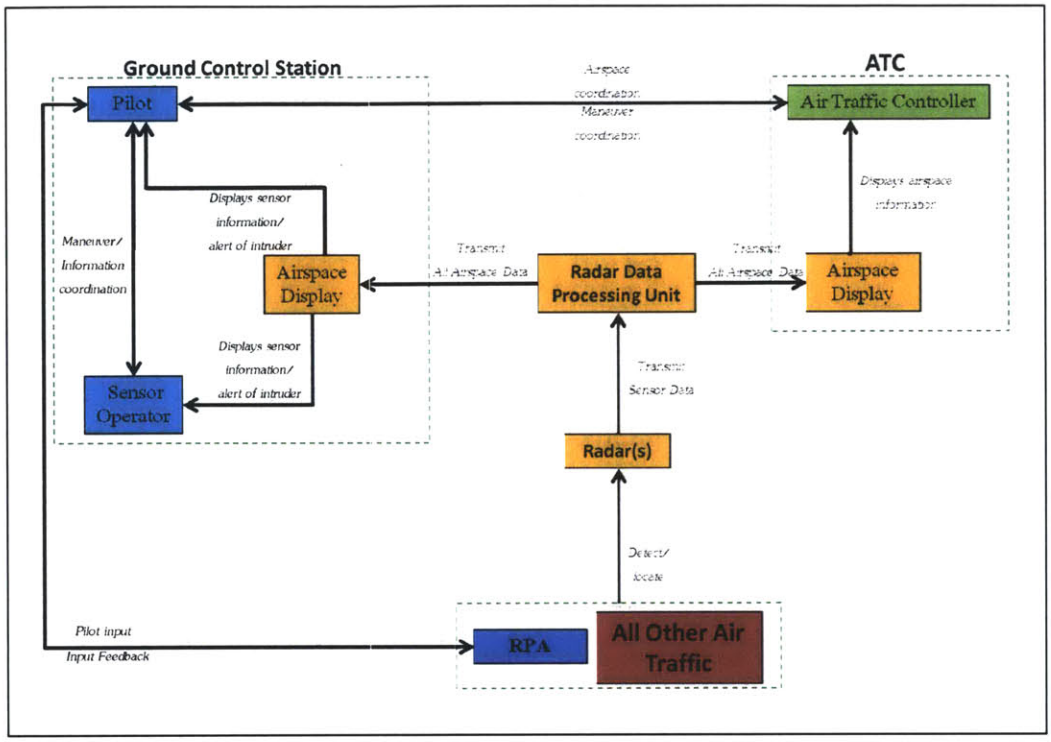


Figure 9: GBSAA Architecture Diagram [2]

From Figure 9, the GBSAA system elements specific to Cannon AFB are divided into major groups: ground control station (light blue), radar data processing (orange), air traffic control (green), RPA (dark blue) and all other air traffic (dark red). The following sections explain the specific elements are included within each major group. In the diagram, the boxes represent the system elements and the arrows represent the element's function and the flow of information or action. The direction of the arrows indicates the direction in which an action or flow of information is taking place. The green dashed lines visually represent how system elements are located in the physical world. The Pilot, Sensor Operator and Airspace display are all co-located within the GCS while the RPA and All Other Air Traffic are all located within the airspace. They are separated into major groups because the elements within the group play a similar role in the function of the overall system even though they are all independent systems.

3.3.1 Ground Control Station

The Ground Control Station (GCS) houses the RPA crew and aircraft control consoles for the purpose of operating the RPA, monitoring the airspace, and communicating with ATC. The GCS provides the hardware for flight planning, situational awareness, and interface to vehicle. The individual system elements within the GSC relevant to the GBSAA architecture are the Pilot, Sensor Operator, and Airspace Display.

The pilot is primarily responsible for aircraft command and control during all phases of flight while remaining vigilant to "Sense-and-Avoid" and maintaining safe separation from air traffic. The pilot controls the aircraft through the aircraft control console. This console consists of a joystick for manual aircraft control and a keyboard/trackball for navigating the various system screens and inputting control information into the system [2].

Input commands are sent through a communication link with the RPA by line-of-sight (LOS) data link. If the communication link is interrupted, procedures will be in place to reestablish communications. A radio intercom system allows the crew to communicate within the GCS and with local ATC to coordinate maneuvers. The pilot is held responsible to make all communications with ATC, but the sensor operator may be directed to complete specific communication tasks if the pilot is too busy with other tasks [2]. Figure 10 shows an example of the aircraft control consoles with the pilot and sensor operator sitting next to each other.

Figure 10: Aircraft Control Console built by General Atomics [30]

The sensor operator is primarily responsible for monitoring air traffic by observing the airspace display mounted beside the primary flight displays. The sensor operator

maintains communication with the pilot about the air traffic shown on the airspace display in order to coordinate safe maneuvers [2].

The airspace display is visible to both the pilot and sensor operator positions and each have the ability to monitor the airspace. The coordination between the two crew members adds a layer of complexity to the concept. Both the pilot and sensor operator will be trained on the use of the airspace display and equipment as well as how to manage crew coordination [2].

The crew members will work together in the following manner. First, if traffic has been identified, sensor operator has the primary responsibility to judge whether it poses a risk to the RPA. The pilot may provide judgment, but also has the responsibility to monitor the RPA status and navigation displays. It may solely be the decision of the sensor operator if the traffic is a threat. Second, both the pilot and sensor operator will determine an appropriate avoidance maneuver, if one is necessary. However, the pilot will make the final decision. Both vertical and lateral maneuvers may be used to avoid traffic. Third, the pilot will perform the maneuver. Finally, the sensor operator will inform the pilot when the RPA is clear of the traffic conflict. If the pilot agrees with that assessment, the pilot will maneuver the RPA back to its mission profile [2].

The airspace display located in the GCS will be a stand-alone display separate from any other flight displays. It displays aircraft locations received from the radar data processing unit. Further details are provided in the radar data processing group in Section 3.3.2.

3.3.2 Radar Data Processing

The radar data processing group detects airborne objects and processes the radar results to provide aircraft tracks that can be displayed to the RPA crew and air traffic controller. This group of systems includes the ground-based radar(s), radar data processing unit, and airspace display.

For Cannon AFB RPA operations, one ASR-8 ground-based radar located at the airfield is used [29]. The use of radar is the primary means by which the pilot will remain vigilant to see and avoid other aircraft along with the assistance of ATC services when necessary. Multiple radar systems can be used together to provide the sensing function of

the airspace, but for this research it is assumed only one radar is used. The radar detects airborne targets that are in range. Detected targets can include aircraft with transponders (cooperative), and airborne objects without a transponder (non-cooperative, e.g. balloons or hang gliders). To ensure all airborne targets are detected, the RPA operations are planned to remain inside the effective radar detection range [2].

The data from the radar will be transmitted to a processing unit. The radar data processing unit will process the data through various algorithms to properly format the data to use for the airspace display. Processing algorithms formulate aircraft location and tracks based on the series of location data provided by the radar. The designers of the algorithms will determine the criteria for the track and location of an aircraft that is considered unsafe for the RPA. The unsafe condition will command the airspace display to provide an alert. The criteria for alerting can be adjusted as technology or regulations are changed in the future. The processing unit will output the properly formatted data to be displayed and command alerts by the airspace display [2].

The airspace display is a monitor that displays formatted track data to illustrate the current location, altitude, and heading of all detected aircraft. When commanded by the data processing unit, the display will provide an alert to the crew to warn of a threatening aircraft. The alert can be a visual and/or auditory alert. It is assumed that the airspace display used within the GCS and Cannon ATC are identical hardware but are separate units in different locations. They both carry out the same functions of displaying information and alerting of a traffic conflict [2].

3.3.3 Air Traffic Control

The air traffic control group monitors and controls the aircraft within the airspace local to Cannon AFB. The human controller directs aircraft to maneuver as necessary to ensure airborne separation. This major group includes the air traffic controller and airspace display located within the Cannon AFB Radar Approach Control (RAPCON) tower.

An air traffic controller has many responsibilities, but for the scope of this architecture diagram, the controller's only considered functions are to monitor the GBSAA airspace display, maintain communication with the RPA pilot, and separate

cooperative aircraft during all phases of RPA operations. The RPA pilot will communicate with ATC through a VHF radio connected to the ground control station. The airspace display in the RAPCON tower will be a stand-alone display separate from any other ATC displays. It displays the airspace information received from radar data processing unit. Further display details are provided in the radar data processing units group in Section 3.3.2.

3.3.4 Remotely Piloted Aircraft

The remotely piloted aircraft is designed to perform reconnaissance missions at medium altitudes with long endurance. The main interacting functions of the RPA in the GBSAA architecture are to communicate with the pilot by receiving commands and providing feedback through sensor feeds. The RPA is also detected by the ground based radar for an accurate airspace picture. The airframe contains the following systems which can have an impact on the system safety:

a. Communication link –The aircraft carries a line-of-sight data link [31]

b. On-board sensor (payload) – capable of carrying multiple sensors including an electro optical (EO) camera. The full motion video from each of the sensors is transmitted back to the GCS to be viewed. The EO camera allows the pilot to observe what is immediately in front and around the RPA [31]

c. Propulsion – turboprop engine [31]

d. Power – aircraft electrical power is generated by the aircraft engine [31]

e. Flight Control – the flight control system provides three-axis aerodynamic stabilization of the aircraft. Flight control commands are transmitted from the GCS to the aircraft via the communication link [31].

3.3.5 All Other Air Traffic

All other air traffic is defined as non-cooperative and cooperative aircraft within the airspace the RPA is operating. The function of air traffic is to be detected by ground based radars.

Cooperative aircraft have an electronic means of identification (i.e., a transponder) aboard and operating, as well as communicate with ATC to coordinate navigation procedures. Non-cooperative aircraft do not have an electronic means of identification (i.e., a transponder) aboard nor have active communication with ATC. The equipment may not be operating due to malfunction or deliberate action [1].

Chapter 4

Safety Assessment Process Application

4.1 Introduction

The Air Force Safety Center (AFSEC) is working with Cannon AFB to build a Risk Management document assessing the operational hazards associated with RPA testing and flight crew training operations in local airspace while transiting to restricted airspace. The purpose of the analysis is to determine if the proposed Ground-Based Sense and Avoid (GBSAA) system is safe. The results of the safety assessment will be presented to the FAA as a part of a COA application. The report will include identified hazards, assessment of the corresponding risk, and documentation of mitigation strategies. This chapter will describe the process used to support the AFSEC in assessing the safety of the GBSAA system and how the information gained from that process is applied to the IM case study.

4.2 Safety Assessment Process

Common safety assessment processes steps are shown in Figure 11 [18].Starting on the far left of diagram, the inputs to safety assessment process include a description of the proposed system change that consists of change elements and external elements. These external system elements are decomposed into interacting and non-interacting elements. The GBSAA system architecture for this research constitutes the proposal change, and was described in Chapter 3.

The safety assessment process is shown by the grey-shaded box at the center of the figure. Included in the process are important sub-processes where decisions are made that influence the safety behavior of a system. These sub-processes include: hazard/risk identification, scoping, detailed assessment & modeling, and mitigation.

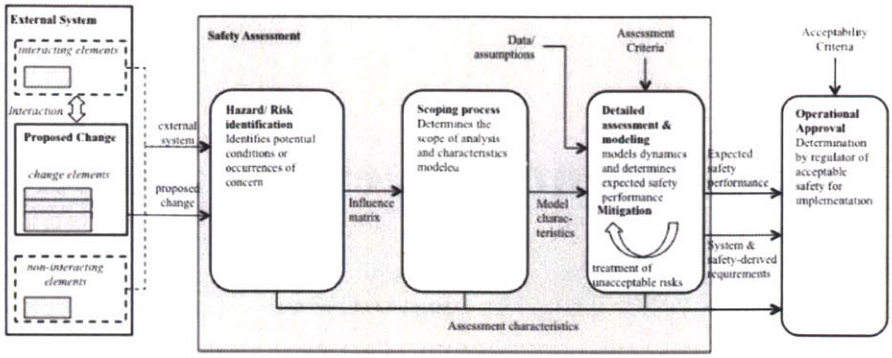


Figure 11: Safety Assessment Process Diagram [18]

Hazard/Risk identification uses the description of the system to determine potential risks and/or hazards associated within the architecture. The result of this process is represented by a formal list of hazards. System experts can be used to build a formal list of hazards that they consider comprehensive and complete. The team of system experts can consist of any personnel or sources that can provide any level of insight into the operation, behavior, or architecture of the system. The application of hazard identification for the GBSAA system is described in Section 4.3.

The safety behavior of a system can be very complex. To better allocate resources to specific areas of concern, the next step in safety assessment is scoping. The scoping process results in an identification of the components for detailed analysis. Scope defines the elements, risks, and conditions that must be included and excluded within the detailed modeling and assessment. The application of scoping for the GBSAA system will be discussed in Section 4.4.

In the process of detailed assessment and modeling, the safety performance of the system is evaluated. Data can be obtained from a variety of sources. For example, operational experience or expert opinion can be used as data to support the assessment. In addition to the data, assumptions are made in the creation and evaluation of the detailed model. Unacceptable safety performance that does not meet assessment criteria is mitigated through safety requirements and various planned strategies. The process of detailed assessment is described in Sections 4.5.

On the far right of Figure 11, the safety assessment produced outputs to support an operational approval decision. The outputs of safety assessment include assumptions made, data used, and modeling approaches. The approving authority determines

acceptability criteria. The criteria are typically defined ahead of time by the authority and the assessment tries to provide adequate results for those criteria.

4.3 Hazard Identification

The first step in safety assessment of Cannon AFB is the identification of hazards related to GBSAA. To identify those system hazards, a team of experts was chosen by the AFSEC that included personnel from: MIT Lincoln Laboratory, MITRE Corporation, Cannon AFB, and the Air Force Safety Center. The experts collected data about the GBSAA system to have an understanding of the proposed operations and focus their knowledge on a specific system, function, or activity. Data collection started with available supporting documents, like the CONEMP, built by the USAF and FAA that provided an understanding of how a GBSAA system worked in relation to the RPA and NAS. After data collection, the team of experts worked together to produce a formal list of hazards.

To identify a hazard, the definition of a hazard must be understood because the identified hazards describe and dictate the safety behavior of a system. A hazard is defined as a set of conditions in the system that could result in harm to personnel or property. Hazards have an associated likelihood, but do not directly have an associated severity measure, as they are not occurrences. There can be several possible outcomes from a hazard which can have different severity levels. A set of conditions or state can only be classified as a hazard if it leads to an event that creates damage or harm to the system or environment. Hazards that result in damage or harm are assigned levels of severity based on the harm associated with them [18].

The hazard list was built by eliciting the expert opinions about the following questions:

1) What are the inputs and outputs to each system?

2) Where do these inputs come from and outputs go to?

3) What function does the system serve?

4) How could this system fail?

5) What are the systems relationships to other systems?

Subject matter experts began by building an architecture diagram (Chapter 3) to represent the GBSAA. With an accurate diagram of the system, the experts could look for hazards have may have been missed or suggest improvements to the system. The diagram provided a focal point for team discussions of functions, failures, and activities as to eliminate confusion about the system.

Using the architecture diagram with forward and backward searches, the list of hazards was created and agreed upon by the assessment team. The forward search for hazards was the process of beginning with system elements and identifying hazards based on the failure or error produced by a particular system element. The backward search began with system hazards or outcomes posed by the system as a whole then traced back to any system element that could lead to the hazard.

One example identified hazard is the airspace display failing to show the crew what is occurring in the airspace. In the forward search, the airspace display can contribute to a hazard by not displaying any information. The backwards search links the hazard of the crew not being able to see the airspace conditions while inside the GCS to the airspace display element. The architecture diagram verifies this hazard because there is a flow of airspace information to the crew from the display, and a break in that flow impacts the crew's ability to safely operate the RPA.

Appendix A contains the full list of hazards identified for RPA operations at Cannon AFB.

4.4 Scoping the Assessment

The scoping process determines the boundary of the safety behavior to be modeled. The scoping process is important in any assessment because it determines the results it can produce. As an example, an FHA is scoped to the appropriate amount of system elements and functions each of those elements. An FHA does not consider the sequence of events leading up to or beyond the failure of a system element. It is only focused on the designed function of a system element. This scope dictates the results because the FHA describes the failure modes in which the system elements may lose their functionality. The FHA does not show how the loss of that function impacts any other system element.

The determined scope of the work completed with the AFSEC assessed the only assess the safety behavior that contributed to the sense and avoid function. For example, the scope of the assessment evaluated the pilot's function of controlling the RPA. The safety assessment did not include the pilot's need to stay awake while operating the aircraft. Mitigation strategies and policies are already in place to handle the example and other out of scope hazards.

Within the GBSAA system architecture, an RPA is the primary system involved. Unfortunately, the RPA has its own set of hazards associated with it regardless of where it is flying. The decision was made to focus on the new hazards produced by flying the RPA in the pubic airspace and using the GBSAA solution, with the understanding that the hazards the RPA inherently brings with its use still have a contribution to the overall safety of the GBSAA solution.

The scope of the assessment was narrowed further through the use of an airworthiness certification. BY legal authority, the DoD certifies the airworthiness of public aircraft, and the FAA recognizes that certification. For the RPA to be considered airworthy, both the aircraft and all of the other associated support equipment of the RPA as already undergone a safety assessment. If any element of the aircraft is not in condition for safe operation, then the RPA would not be considered airworthy [1]. If the RPA is airworthy, then the aircraft elements are assumed to be able to execute sense and avoid maneuvers.

4.5 Detailed Assessment and Modeling

To assess the GBSAA system at Cannon AFB, the AFSEC chose between many models and safety assessment tools. The AFSEC chose to model the system with commonly understood and widely used methods of a Functional Hazard Assessment and Fault Tree Analysis to support the Risk Management document.

4.5.1 Functional Hazard Assessment Application

Using the systems architecture described in the Chapter 3 an FHA was built using SAE ARP 4761 as a guidance document [19]. The FHA results are provided in Appendix B as a reference. The FHA models the system elements included within the architecture

through a functional description of each element and how those functions could fail. The failure condition of a function may or may not lead to a hazard.

The FHA was completed to verify and confirm that all hazards were identified for the GBSAA system. Each of the identified failure conditions was compared to the formal list of hazards to examine if any failure condition that lead to a hazard was missed. After examination, each failure condition was successfully paired by an identified hazard and that provided confidence and verification to the team of experts that all operational hazards had been identified.

4.5.2 Fault Tree Analysis Application

The FTA is a top-down process that starts with a high level hazard and breaks the system down into faults of elements that contribute to the overall hazard. The AFSEC began with the most critical hazard of mid-air collision (MAC) and described all the faults that could contribute to that condition. The FTA for the GBSAA system is included in Appendix C.

The FTA modeled the GBSAA system by describing the contributing elements to each single fault event that contributed to a MAC. By decomposing the contributing elements to particular hazardous conditions, insight is gained as to how each element impacts various hazards. Some elements may only impact one hazard while other elements may impact several different hazards.

In addition to seeing how many hazards an element influences, probabilities of failure can influence how the system element contributes to a hazard. The assigned probabilities can provide quantitative results to determine the risk of different outcomes through the tree. The "or" and "and" gates of the FTA structure determine how the mathematical functions operate in relationship to each hazardous condition. The probability of a hazardous condition at any level of the tree can be computed using the mathematical functions and failure probabilities of the elements that are decomposed below the hazard of focus. The entire tree will ultimately provide a risk value to the outcome listed at the highest level of the tree. For the example shown in Appendix C, quantitative probabilities could be used to determine the overall probability of a MAC occurring.

The mathematical functions of the "or" gate or an "and" gates can describe the criticality of a system element in relationship to the outcome. If a hazardous outcome can occur due to one system failure in an "or" situation rather than requiring a combination of failures, stronger mitigation may need to be implemented.

4.6 Discussion of the Safety Assessment Completed for Air Force

The Hazard Identification process is limited by the human personnel that identify and build the formal list. First, the selection of those included on the team of experts creates a limit of knowledge. Experts are selected based on the knowledge of the existing RPA systems and proposed GBSAA solution. Some individuals may also have experience and knowledge with prior safety assessments of other RPA operations. The Air Force Safety Center intended to have experts with broad general knowledge and specific expertise knowledge on many subjects that can be related to the GBSAA assessment. Each person may have slightly different backgrounds of knowledge, but that diversity is purposeful and can leveraged to assess the system with different perspectives. The different perspectives helped the team of experts logically identify hazards and provide confidence that no hazards are missed due to a lack of knowledge or perspective.

Limits to human knowledge constrain the hazard identification process. Humans are biased to the knowledge they have and may not be able to predict a situation that has not occurred in the past or is extremely rare. For the extent of the research in this thesis, it is acknowledged that humans may not be able to identify all possible hazards or predict all functions of every system element. This limitation is an acceptable part of the process and must be understood for the extent of the safety assessment process. It is not a flawless process, but the humans have the best intentions to assess the system as honestly as possible based on their knowledge and experience in the field.

Scoping the list of hazards proved to be complex because two distinct sets of hazards appeared. The team of experts identified a set of hazards that included a mid-air collision, but also identified a set of hazards resulting in traffic conflicts without collisions. The hazard of a traffic conflict does not result in damage to any system and only requires action from the pilot and sensor operator to adjust flight plans. The results of a mid-air collision hazard are much different because it may cause the loss of the

aircraft and possibly human lives. The difference in the hazard condition and separate outcomes gave the team of personnel reason to create a separate the list of hazards for the two conditions.

The detailed models shown in the FTA and FHA expose a decomposition challenge. Decomposition is the act of breaking the whole system down into system elements. Each level of decomposition can grow the size of the model exponentially, so the challenge is to keep the model from getting too large while making sure the model is complete. No two models are alike, and there is no standard for when a model is considered complete. A general guideline is to decompose the system to a level of detail the author of the model determines as adequate. The author may have to defend or explain the decision behind the level of detail chosen.

Chapter 5

Influence Matrix Framework

After the safety assessment was performed with AFSEC to construct the Risk Management document the same information provided by Cannon AFB was applied to the influence matrix (IM) framework. This research task was performed for this thesis to evaluate insights that can be drawn about the detailed model of the system and the described safety behavior compared to traditional methods.

5.1 Influence Matrix Framework Motivation

Motivated by the scoping and detailed assessment challenges discussed, past research conducted at MIT was applied to the Cannon AFB safety assessment. The influence matrix framework has shown its ability to present a condensed safety model focused on the relationships system elements and hazards [18].To learn more about the characteristics and results of the framework, it is applied to the GBSAA system independently from the traditional methods used by AFSEC. The IM reused the system description and identified hazards that have already been defined using the work explained in Chapter 3 and Section 4.3, respectively. This chapter will explain how the IM framework is scoped and built using the GBSAA system information.

5.2 Influence Matrix Framework Description

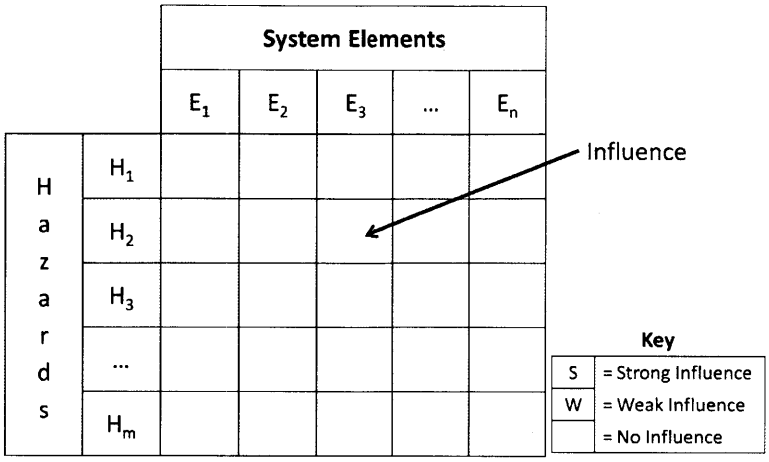


Figure 12: Example Influence Matrix [18]

The IM describes the relationship between system elements and hazards by coupling them together based on the influence each element has on that particular hazard. The magnitudes of influence will be arranged in the form of an "m x n" influence matrix shown in Figure 12. The "m" rows of the matrix denote hazards (H_m), and the "n" columns of the matrix denote system elements (E_n). Each cell of the matrix is the influence of the corresponding element to that hazard or risk. Determining the level of influence requires judgment on behalf of the safety assessor and that will be explained in more detail in Section 5.3.

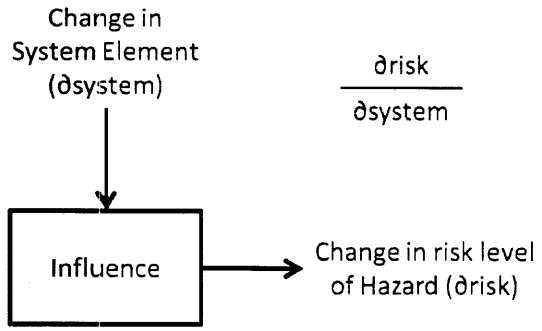


Figure 13: Definition of Influence [18]

The influence is defined conceptually in Figure 13. Influence is a measure of the change in risk level of a given hazard (∂risk) due to a change in the system element (∂system). The determination of influence is normally based on the judgment of a safety assessor. The partial derivative in Figure 13 defines the amount risk changed per a

change in the system element. It should also be noted that a change in a system element could also change the severity associated with a risk. This dynamic is not captured in the framework and would require further refinement in future applications of influence.

Influence represents the ability to affect a level of risk based on the functions or actions taken by a specific system element. System elements can be aspects of change without explicit parameters relating it to risk [18]. An example of a system element change is flight crew performance. While their performance clearly influences some risks of hazards like pilot induced oscillations, failure to follow procedures, or incorrectly land the aircraft, the risks may not be parameterized. The training each crew member must receive teaches the crew how to properly act and function within the system as a whole. Without that training, crew performance may change which has an influence on risk. To capture the element of change within the IM framework, the partial derivative value is defined conceptually and represents the change on risk levels based on a change in behavior of an element, the crew.

The changes do not necessarily have to be continuous or parametric. Influence as defined here also does not have a positive or negative sense [18]. Influence may represent that changes to a system element can expected to only increase risk level, only reduce risk level, or increase or reduce risk level depending upon the properties of the element. Influence will be coded based on its absolute magnitude, as described in the following section.

The influence matrix representation assumes a linear relationship between elements and risks of hazards. Each influence value is constructed independently of other system elements. Although this is a limitation of the framework, it does not imply that expected safety performance of a system is the result of a linear combination of the safety performance of individual elements [18]. Interactions between elements will exist in a real system. The complexity in interaction is captured in the detailed modeling and assessment process, when expected safety performance is evaluated in detail.

5.3 Influence Matrix Framework Application

The primary goal in of the IM framework analysis is to identify all possible system interactions and accurately determine the influence each system has on a

particular hazard. The secondary goal is to use that information to provide a safety assessment method that can assist in determining mitigation and evaluation strategies.

Using the Cannon AFB GBSAA formal list of identified hazards and the system elements defined in the architecture diagram, the columns and rows are populated for the influence matrix in Figure 14. With the matrix axes populated, a level of influence must be determined for each cell in the matrix. The levels of influence for this matrix are qualitative with three possible options: no influence, weak influence, and strong influence.

No.	Hazard	System Elements								Key
		Radar(s)	Radar Data Processing Unit	Airspace Display	Pilot	Sensor Operator	All Other Air Traffic	RPA	Air Traffic Controller	S = Strong Infleunce W = Weak Influence *blank* = No Influence
HA1	Airspace display failure, leading to undetected intruder and NMAC	W	W	S		W	W			
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC	S	S				W			
HA3	Radar degradation, leading to undetected intruder and NMAC	S					W			
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC				W	S	W			
HA5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and NMAC	W	S	W			W			
HA6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to NMAC	W	S				W			
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	W	S	W	S	W	W			
HA8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a NMAC	S	S	S			W			
HA9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and NMAC	S	S	S			W			
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	W	S	S	W			
HA11	RPA is not able to maneuver in time to avoid a potential NMAC				W		W	S		
HC1	Airspace display failure, leading to a traffic conflict	W	W	S		W	W			
HC2	Communication failure between radar and radar data processing unit, leading to undetected intruder and a traffic conflict	S	S				W			
HC3	Radar degradation, leading to undetected intruder and a traffic conflict	S					W			
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict				W	S	W			
HC5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and a traffic conflict	W	S	W			W			
HC6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to a traffic conflict	W	S				W			
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	W	S	W	S	W	W			
HC8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a traffic conflict	S	S	S			W			
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict	S	S	S			W			
HC10	Inability to communicate with ATC, resulting in traffic conflict				S	S	W		S	
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing				S					
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway				S	W				
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.				S	W				
HN4	Crew loses situational awareness of RPA status, leading to NMAC				S	S	W			
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict				S	S	W			
HN6	Loss of aircraft power due to engine failure that results in an off field landing, resulting in aircraft damage							S		
HN7	Loss of aircraft power due to electrical failure that results in an off field landing, resulting in aircraft damage							S		
HN8	Catastrophic aircraft system failure that results in a crash and ground fatalities							S		
HN9	Loss of datalink that results in a near-mid-air-collision (NMAC)						W	S		
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities				S	W		W	S	
HN11	Uncommanded altitude or course deviation that results in a NMAC				S	W	W	S	S	
HN12	Pilot commands unsafe maneuver that results in a NMAC				S	S	W			
HN13	Loss of datalink that results in a traffic conflict.						W	S		

Figure 14: Influence Matrix Framework

As shown in Figure 14, if the influence level is a strong influence it is signified by an "S", a weak influence is a "W" and no influence is a blank box. Using the partial derivative in Figure 13, influence can be described as the value of changed risk resulting from a system element change. The influence could be determined quantitatively based on failure rates and a fault tree, but for this research, quantitative approaches were not readily available. A qualitative framework is expected to show similar conclusions. If a given influence is strong, a large magnitude change in the associated risk will result from a change in the behavior of the system element. Influence is weak when a small magnitude change in the associated risk is results from a change in system element behavior. Weak influences can often act indirectly or in combination with other elements in the system. Blank boxes indicate no influence between the system element and associated risk level for that specific hazard. In this case, there is no relationship between the system element and hazard and do not change the magnitude of risk of that hazard.

Determining the difference between strong, weak, or no influence, requires some judgment. A decision was made to place thresholds for each influence level and those thresholds had to remain consistent for the entirety of the model. To explain the thresholds between the levels of influence the hazards are categorized into three general modes in which an element may influence a hazard: loss of element function, faulty/incorrect input data, and misinterpretation of element behavior.

The first mode of system failure is a loss of functionality in an element. For hazard HA1, "Airspace display failure, leading to undetected intruder and NMAC," the airspace display element has a strong influence on system failing to function. The display element can have a complete loss of system function that is not created or caused by any outside element. The airspace display screen could go blank and not display any information to the sensor operator. The display could also be set up incorrectly and lose its ability to function. This change in system behavior results in a high magnitude of risk that is represented as a strong influence in the matrix.

The strong influence has also been reflected in the FHA and FTA. In the FHA, the functions of the airspace display are to provide pilot and sensor operator with sensor information describing the local airspace and provide both visual and audio alerting to pilot and sensor operator. The failure to perform or incorrect performance of these

functions directly influences the hazard of "airspace display failure." In the FTA, under the fault of display failure are the direct system failures as listed above for the strong influence of the hazard.

The second mode of failure is incorrect data input. There are several systems that have an input for hazard HA1: the radar(s), radar data processing unit, and all other air traffic. The reason for their influence is because the radar and data processing unit can affect the state in which the display operates which could then lead to a failed display even though the display is functioning correctly. The change is system behavior of the radar and data processing unit results in a small change in risk because they both have to contribute to the hazard. These elements have a secondary influence because one system failing by itself should be noticed but not drastically change the risk level. All other traffic is a weak influence because of the potential for a NMAC, but the element does not influence the airspace display failure. Without the presence of the air traffic this hazard would not exist.

The radar and processing unit can send improper data to display generating a false picture, but the display could be functioning correctly with the wrong information. This weak influence is generated by the similar functionality of the radar data system group described in Section 3.3.2. The additional step beyond the display just failing independently creates a smaller change in risk and the influence, which is represented as weak in the matrix. In other words, the change of the radar, data processing unit, or sensor operator has a low magnitude of risk associated with each change in system element. Assuming all remaining system elements are functioning as designed, it is assumed then the operator will be notified or aware of a data error or setting change. The change in display behavior has a weak influence on the hazard risk because the display may not lose complete functionality, but the degradation increases the risk of the hazard occurring.

The third mode of failure for the system in exposed in the misinterpretation of the system behavior. For hazard HA1, the display could have correct data and be working properly, but the settings could fail to correctly show the data to the sensor operator. This could occur if the sensor operator manipulated the display settings or improperly read the information on the display because the display in zoomed out too far on the local area.

This is a contributing influence to the hazard, and by itself only changes the magnitude of risk by a small amount, therefore, it is a weak influence.

The weak influence can again be seen in the FHA and FTA. The function of the sensor operator is to "Maintain situational awareness of airspace," and incorrectly performing that function (misreading display) influences the hazard of airspace display failure. If the information isn't being read correctly, the display is contributing to the confusion of the operator. In the FTA, the display failure can lead to a false reading or incorrect decision. The pilot or sensor operator contributes to this hazard, but each is not the only influencing element. The function of the processor is to "Transmit data to Airspace Display." The failure to do so or sending corrupt data can lead to an incorrect display picture, but enough information could get through to the sensor operator to not create a hazard. The display itself may not fail, but the information could give that appearance to the sensor operator. In the FTA, the processor error is on an equal level to the display failure meaning they are both contributing causes to an uninformed pilot, but not a direct cause to a display failure itself. This shows some influence but not a direct or strong influence. This situation also occurs for the radars or sensors within the FTA, again creating a situation for weak influence.

The remaining system elements do not change the magnitude of risk above the threshold for weak influence because they are completely isolated from the hazard. The elements either located within another major group of the architecture or the element is more than two informational steps away from the strong hazard influence, so it will not have a large enough impact on the risk when the element behavior changes.

To complete the entire influence matrix the same judgment process and philosophy used for hazard HA1 was maintained to populate the influences of the remaining elements.

5.4 Discussion of Influence Matrix Application

Weak influence can be caused by a data flow of poor information. For example, if a display does not appear to be working properly, then it does not always mean the display has lost full functionality. Anything in the stream of the data could be malfunctioning, so each element within the data stream has a broad influence on all elements reliant on that

information flow. The radar scans the airspace and sends information to the processing unit, which provides data to the display. The display is then monitored by the sensor operator and pilot that control the RPA operating in the airspace. The RPA's position is again monitored by the radar. The pilot also coordinates with ATC to influence the other aircraft in the airspace, which is all detected by the radar.

The process discussed above illustrates a closed circuit in the flow of information. This flow of the information through all elements creates a broad influence and forces the assessor to use judgment to determine the threshold for what is considered a weak versus non-influencing element. The threshold was determined by where a system has an interaction within the same major group that contains the strong influence on the hazard. Hazard HA1 was described in this fashion in Section 5.3.

(this page intentionally left blank)

Chapter 6

Clustering Application

Motivated by the scoping and detailed assessment sub-processes, this chapter will apply clustering techniques to the influence matrix framework for further analysis. This chapter will document the insights gained from using clustering techniques and how those insights help support a better understanding of safety assessment methods and the Cannon Ground-Based Sense and Avoid (GBSAA) functionality.

6.1 Motivation to Explore Clustering Techniques

Complex interactions created by a complex system provide a need for a safety assessment method that can accurately model the system and describe safety behavior. This scoping process can be resource intensive with numerous system elements because of the large amount of interactions between them. Scope of the FHA and FTA methods require the user to define all system elements and functions to a high level of detail in order to assign likelihoods to a final outcome. With a highly complex system, the FHA and FTA may produce extremely large models that may not be physically able to define and test every element in every possible condition. Condensing the scope of the model or determining how to focus recourses may offer advantages to describe and assess safety behavior of complex systems.

In past research conducted at MIT, the influence matrix framework applied a notional clustering technique that provided useful insights for scoping a safety assessment. The research stated that future research can be conducted "...to develop automated tools to analyze sets of hazards with structured forms of influence" [18]. To develop automated tools, a formalized method of clustering can be established for the IM framework. To determine the proper ways to formally cluster the matrix, literature was reviewed to find similar assessment tools using formal clustering methods.

Clustering hazards may help reduce the amount of recourses spent on analyzing individual hazards or system elements by analyzing them in groups. It is expected that the

IM framework will be able to use the clustering techniques due to its matrix format and similarity to other another matrix safety assessment method.

The IM framework is similar to a Dependency Structure Matrix (DSM). It models relationships between system elements in a matrix format. Therefore, clustering approaches for DSMs were explored. The similarities and differences between the DSM and IM are important in understanding clustering techniques that were originally designed to be applied to the DSMs. Many of the clustering techniques depend upon the unique structure of the DSM. While the IM does not have the same physical characteristics as the DSM, the similarities between them will be explored with the objective of choosing a clustering technique that will be applied to the IM. The next two sections of this chapter briefly describe the DSM format and introduce clustering techniques to further describe the motivation behind this type of research.

6.1.1 Dependency Structure Matrix Format

The Dependency Structure Matrix (DSM) is a matrix formatted method for describing complex system interactions. It has three similar characteristics to the IM framework. The first is the goal of each method to identify interactions and relationships in the system to recommend where to focus analysis. The relationships help expose safety behaviors of the system like potential critical systems or interoperability issues [32]. The second common characteristic is that the assessed system is decomposed into elements that are determined as important for system functionality. Those elements are then listed on the axis of each matrix. The third is the description of the relationships occurring within the system elements. The description of a relationship in the DSM or IM may be binary, but that is not required. One might use a number to indicate the critical relationships, strength of the relationship, risk, and many other metrics. Both methods can even describe more than one interaction. The matrix format can determine indirect couplings and dependencies as well as calculate their impact on the entire system [32].

The main difference between the DSM and IM is how the relationships are captured. For the DSM, the relationships describe whether or not two elements interact with each other as a pair. As a notional example, Figure 15 shows a DSM with system elements A_1 through A_7 on both the vertical and horizontal axes. The boxes in the matrix

included a check mark to indicate if the paired elements interact or not. Each check mark is an individual interaction pair. A diagonal grey line in the DSM is created because the system element does not create an interaction pair with itself. As described in Section 5.2, the relationships of the IM describe if the system element interacts with a particular hazard.

Both of the methods are two-dimensional, but the size of each matrix is different as a result of the relationships being described. In Figure 15, the DSM uses a matrix that is defined by "A_x" system elements on each axis. The size of the matrix then becomes "x^2." As described in Section 5.2, the size of the IM is "m x n."

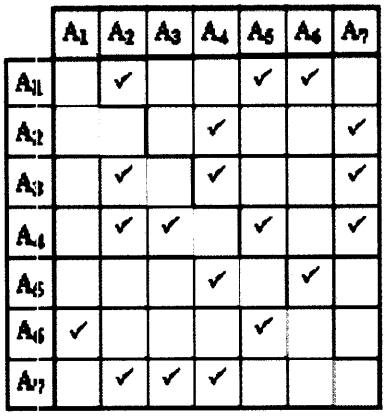


Figure 15: Dependency Structure Matrix [32]

6.1.2 Clustering Techniques

The objective of DSM clustering is to use the system element individual interaction pairs and regroup those pairs into a group that defines a relationship at a high-order of abstraction. This so-called higher-order relationship is a broader relationship within the group that is common among all included elements. The elements will have similar interactions, influences, or properties in their behavior as they serve a function within the overall system [33]. An example of this would be the human circulatory system. The elements of the heart, veins, arteries, and capillaries each have individual interactions with other parts of the body, but the high-order relationship is that all of them transport blood.

DSM clustering techniques have been shown to be useful in identifying architectural improvement in organizations and product design and development [33].

Clustering can help to better understand complex interactions within a system architecture. Then, an assessor can use the clusters to assess the system in a condensed version to impact future planning and assessment.

Clustering techniques extract further information about the system architecture. Clustering informs the assessor by identifying elements that behave similarly or differently in comparison to the rest of the system. Information from that behavior can be useful for test prioritizing and risk mitigations strategies. The clustering technique provides the opportunity for the assessor to better understand how the complex system elements work together to create a larger system entity. Some system elements may have more interactions than others. The clusters can help system assessors focus attention on specific elements rather than viewing every possible interaction combination. The clusters also draw attention to elements that are identified as acting independently of all other elements. Those independent elements may be easily looked over or forgotten otherwise. A cluster will highlight a system element interaction where it is not expected or vice versa.

There are several formal clustering techniques available to use based on several approaches in literature ([32], [33], [34], [35], [36], [37], [38], [39], [40], [41]). Many potential formal clustering processes were identified: mathematically based, process based, architecture based, or any combination. A mathematical cluster technique uses a formula to rearrange the system interactions based on measured parameters and produce an optimized result. Such techniques can use weighting and relationships counts to find the most highly involved system elements. A process clustering technique rearranges the elements based on a specific set of steps. An architecture based technique clusters interactions by similar functioning system elements or by elements that directly communicate with each other. Each of these methods achieves a similar objective of creating clusters.

The objective of each cluster is to maximize interactions within the cluster while minimizing interactions between the individual clusters. This results in clusters that contain the most similarity in elements functionality in one cluster. If there is too much interaction between two clusters, then those may need to be combined. If they do not interact at all, then the clusters are formed correctly. The assessor must use judgment to

determine when clusters have a level of interaction where it is not possible to completely separate the clusters.

It has been suggested to minimize the size of the clusters in order to identify clusters that only contain elements that behave exactly the same [35]. This objective may be counterproductive for the purpose of clustering for safety assessment. If the clusters are minimized in size, then there may be too many clusters for the assessor to determine which are the most important.

Other work suggests that highly interactive system elements are assigned to a "controls cluster" that influences all clusters [35]. This technique could be useful for systems that have control systems that monitor all elements within the architecture.

6.2 Selected Clustering Technique for Influence Matrix

Each of the previously discussed clustering techniques exposes that each system may have unique architecture properties that can be clustered differently based on the judgment of the assessor. To inform safety assessment, key objective in applying clustering are to maximize interactions between hazards and system elements within the individual cluster while minimizing interactions between the clusters of hazards. Highly interactive elements within a cluster functionally groups similarly behaving elements for safety assessment. The secondary objective of the clustering technique is to identify clusters that are large enough to ensure no influences are left isolated. Removing isolation eliminates the need for special consideration of resources to be used on just one influence rather than looking at a group of hazards together. An efficient use of time and resources analyses groups of hazards and systems rather than just one at a time.

The format of the IM is that each column represents a system elements and each row is a hazard. By this arrangement, there can be two possible types of clusters. There can be clusters of system elements that influence similar hazards or clusters of hazards influenced by similar elements. For the process of safety assessment, the clusters of hazards influenced by similar elements are expected to provide more insight into the safety behavior of the overall system. The clusters of hazards are expected to show which hazards are more critical to the safety of the overall system than others. Critical hazards will be those that are influenced by the most system elements because those hazards will

have the most opportunities to be influenced through mitigation strategies or controls that reduce risk. The clustering of hazards provides an opportunity for the safety assessment to mitigate groups of hazards that are similarly influenced rather that mitigating each hazard individually.

The small size of the influence matrix constrained the selection of a specific clustering method. Because the influence matrix only contains eight system elements and thirty-four hazards, visual inspection and manipulation was judged to be an adequate technique. Literature suggests this is appropriate for small or sparse matrices [35]. The application of clustering by visual inspection to the Cannon GBSA architecture is a specific process that will be discussed in detail further in Sections 6.2 & 6.3. First, advantages of visual clustering will be discussed further below.

No single clustering approach is simple, but the visual manipulation allows the assessor to quickly evaluate the results of clustering by seeing exactly what hazards are being grouped together or left out. Reordering rows and columns allows the assessor to build a configuration that optimizes the matrix to gain specific insights about the overall system. Any influences not included in a larger cluster will be noticed. This isolated influence will require special attention and verification. The assessor will have to consider adding the influence into a cluster, if possible, or it must be dealt with separately. It must not be ignored, but be reassessed and analyzed. A step by step visual process will be developed for the IM framework with the expectation that clusters will be identified consistently.

The step by step process will be used several times with different central system elements. The objective of this approach is to determine if the clustering process used produces similar or different results when focused on different central system elements. The starting influence matrix will be the same, but if visual manipulation is used, one assessor may choose to focus on a specific element that is different from the element another assessor chose. The comparison of results is expected to produce insight into how the elements interact and how effective the use of visual manipulation is for a clustering technique. It is expected that the different central elements will affect the way hazards cluster together.

It is expected that some system elements will influence more than one cluster of hazards. This interaction between clusters will be useful to recognize certain elements that are contained in more than one cluster. Simply keeping a count of how many clusters a system element is contained in will show the relative influence level the element has on the overall system.

Before applying the detailed clustering technique, a basic use of visual manipulation shows how the process is expected to provide results. A part of the clustering technique is architecture based by physically separating similar functioning components. In Figure 16, the system elements have been separated to reflect the major system groups defined by the architecture diagram described in Chapter 3. These major groups are physically separated by element functions. Grouping elements by major system group shows how certain hazards look to only be influenced by a single major group of elements while others are influenced by multiple major groups. This can be expected because related system elements within a major group serve similar functions, therefore, influencing similar hazards. This topic will be readdressed later in the evaluation of each clustering process.

		Radar Data Processing Major Group			GCS Major Group		Major Group	Major Group	Major Group
No.	Hazard	Radar(s)	Radar Data Processing Unit	Airspace Display	Pilot	Sensor Operator	All Other Air Traffic	RPA	Air Traffic Controller
HA1	Airspace display failure, leading to undetected intruder and NMAC	W	W	S		W	W		
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC	S	S				W		
HA3	Radar degradation, leading to undetected intruder and NMAC	S					W		
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC				W	S	W		
HA5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and NMAC	W	S	W			W		
HA6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to NMAC	W	S				W		
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	W	S	W	S	W	W		
HA8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a NMAC	S	S	S			W		
HA9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and NMAC	S	S	S			W		
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	W	S	S	W		
HA11	RPA is not able to maneuver in time to avoid a potential NMAC				W		W	S	
HC1	Airspace display failure, leading to a traffic conflict	W	W	S		W	W		
HC2	Communication failure between radar and radar data processing unit, leading to undetected intruder and a traffic conflict	S	S				W		
HC3	Radar degradation, leading to undetected intruder and a traffic conflict	S					W		
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict				W	S	W		
HC5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and a traffic conflict	W	S	W			W		
HC6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to a traffic conflict	W	S				W		
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	W	S	W	S	W	W		
HC8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a traffic conflict	S	S	S			W		
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict	S	S	S			W		
HC10	Inability to communicate with ATC, resulting in traffic conflict				S	S	W		S
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing				S				
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway				S	W			
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.				S	W			
HN4	Crew loses situational awareness of RPA status, leading to NMAC				S	S	W		
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict				S	S	W		
HN6	Loss of aircraft power due to engine failure that results in an off field landing, resulting in aircraft damage							S	
HN7	Loss of aircraft power due to electrical failure that results in an off field landing, resulting in aircraft damage							S	
HN8	Catastrophic aircraft system failure that results in a crash and ground fatalities							S	
HN9	Loss of datalink that results in a near-mid-air-collision (NMAC)						W	S	
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities				S	W		W	S
HN11	Uncommanded altitude or course deviation that results in a NMAC				S	W	W	S	S
HN12	Pilot commands unsafe maneuver that results in a NMAC				S	S	W		
HN13	Loss of datalink that results in a traffic conflict.						W	S	

Figure 16: Influence Matrix separated by Major System Groups

6.3 Clustering Technique Application

The clustering technique is divided into two distinct processes of rearranging the hazards and system elements of the matrix and identifying clusters based on the results of the rearrangement. A detailed explanation of the matrix clustering technique in a step-by-step example is included in Appendix D.

6.3.1 Rearrangement Process

The application of the clustering technique begins by re-ordering the system elements so the central element is in the farthest left column, E_1 in Figure 17. With the central element established, the goal is to establish clusters of hazards based on system element behavior similar to that of the central element. The hazards influenced by the central element are then arranged so the hazard that is influenced by the least amount of other systems is placed at the top of the matrix and the most amount of other systems at the bottom of the central element hazards. For example, the hazard located at the top is only influenced by the central element. The next hazards should be arranged from least to greatest amount of other system elements influencing those hazards until all of the hazards that the central element influences are listed at the top of the matrix.

The reason for ordering the hazards by the least number of influencing elements located at the top of the selection and the hazards influenced by the highest number of elements are at the bottom is to centralize the highly influenced hazards. The least influenced hazards will only include the central element while the more influenced hazards will include other elements. This priority method brings highly influenced hazard up from the bottom of the IM which will help further centralize the most influenced hazards in the center of the IM and the least influenced hazards will be pushed to the extreme ends of the IM.

Next, looking horizontally across the matrix at only those hazards the central element influences, the assessor identifies the element that most closely influences the same number those hazards already identified and moves it next to the central element. The priority arrangement technique from the previous step aides in selecting the element

with the most similar behavior because it will have an influence located closer to the top of the matrix than the other elements.

These steps are repeated several times until the hazards and elements have run out of available columns and rows to move into. The steps of rearranging the hazards influenced by the primary system result in a triangle-type pattern shown in Figure 17. (grey triangle). The triangle shape is established by rearranging the system elements so the elements that influence most similar hazards are located to the left of the matrix and those located to the right are the most different elements when compared to the central element. This triangle-type rearranging prioritizes the hazards that have those most amount of influence from other systems to be moved closer to the center of the matrix. The most influenced hazard by system element count will be located at the bottom of the triangle. This high count of influence may not be the most influenced hazard in the system overall, but it is the most influenced hazard that includes the central element.

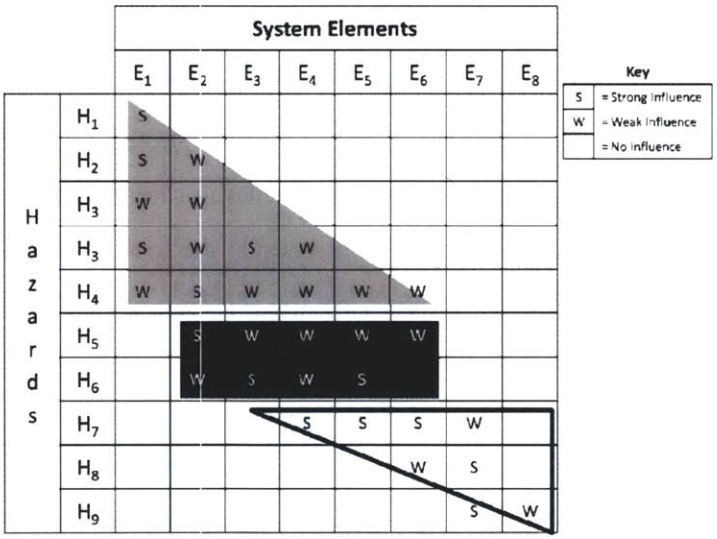


Figure 17: Rearrangement Shapes

As system elements are rearranged to concentrate similar influences on hazards, the clusters of hazards are rearranged to group hazards that are influenced by the same system elements. In Figure 17, the black box shows the concentration of hazards that are influenced by the same high count of system elements identified by the prioritization of the hazards for the central element.

As the rearranging process continues, those hazards and elements that are influenced and behave similarly to the central element hazards are rearranged towards the

top and left of the matrix, while those elements and hazards that influence and behave differently move towards the bottom and right of the matrix (outlined white triangle in Figure 17). This upside-down triangle effect is the result of grouping the most similar system elements and hazards to that of the central element. As the similarly influenced hazards are grouped together at the top and left, the unalike systems are pushed to the right and the differently influenced hazards are pushed to the bottom.

The resulting clusters indicate that a detailed assessment of those hazards and elements behaving similar to the central element is warranted, while abstracting those elements unrelated to the central element. Additional, the most influenced hazards by system element count are located at the bottom of the primary triangle. This results in the most influenced hazards being pulled to the center of the matrix. The centering of the most influenced hazards forces those hazards with only a few connections that do not include the central element to the bottom of the matrix.

The rearrangement process functions to describe the system from the perspective of the central element. The system elements at the bottom of the upside-down triangle are the least interacting with the central element and the hazards it influences. Therefore, those least interacting elements have indirect influence on the central element. This can allow the assessor to view those elements as more abstract. The assessor may group the hazards they influence with less detail because from the central element's perspective, they all behave similarly different and they have that indirect influence the central element.

The baseline influence matrices were rearranged based on three different central elements. The first central element selected is the pilot because the pilot is expected to be the most influential human element within the GBSAA system. The pilot has the most human interactions with other system elements by communicating with the sensor operator, air traffic controller, RPA, and viewing the airspace display. Significant safety mitigations and controls are therefore focused on ensuring pilot performance in the operating concept. The second central element is the RPA because the RPA is the focus and main concern for the GBSAA system. The safety of the RPA is critical, and without it being flown in civil airspace there would be no need for the GBSAA system at all. The third central element is the radar because the radar is required for the GBSAA system to

function. Without the radar, no aircraft would be detected, limiting the ability of the RPA to sense other aircraft in the area which is the primary concern of RPA operations in the NAS.

The shapes in Figure 17 are not the clusters, but shapes only to aid in visually observing how the hazards and system elements are rearranged. A step-by-step explanation of the matrix rearrangement with pictured examples for each step is included in Appendix D. Appendix D only uses rearrangement of the IM with the pilot selected as a central element. The rearrangement based on the RPA and Radar central elements are not explained in such detail. Once the rearrangement of the IM is complete, the cluster identification begins.

6.3.2 Cluster Identification

As explained in Section 6.2, clusters are defined as groups of hazards that are influenced by similar system elements. Each cluster can be visually identified as a group of hazards in rows influenced by a set of system elements across columns. Starting at the top of the list of hazards, each cluster can be differentiated based on the different set of system elements that influence each hazard.

The primary objective of clustering is to maximize the number of influences included in a cluster. This objective can be restated to create clusters that include as few non-influenced or empty boxes as possible. The secondary objective is to create large enough clusters so no influences are left isolated. This section will present a few examples of identified clusters from the IM with the pilot as the central element. The remaining detailed identification of all clusters for the IM with the pilot as the central element is explained in Appendix D after the rearrangement steps.

The first hazard in Figure 18 is a single cluster with a 1 x 1 (rows x columns) dimension. This cluster is a human flight control hazard that only contains one hazard that is influenced by one system element. This satisfies the primary goal to create a cluster that maximizes interaction because the single hazard is only influenced by one element and contains no empty boxes. This cluster successfully functions as producing a grouping of hazards that have similar system behavior.

		System Elements							
No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S	W						
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S	W						
HN4	Crew loses situational awareness of RPA status, leading to NMAC	S	S	W					
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict	S	S	W					
	Pilot commands unsafe maneuver that results	S	S	W					

Figure 18: First Cluster with Pilot as Central Element

Moving downward from the first cluster, the next influence cluster is identified in Figure 19 as a 2 x 2 cluster where only two hazards are influenced by the same two elements. This cluster defines the hazards that occur due to RPA crew procedures for departing or arriving at the airfield. The cluster maximizes interaction as it does not contain a single empty box and it functionally produces a group of hazards that have similar system behavior.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S	W						
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S	W						
	Crew loses situational awareness of RPA status,	S	S	W					

Figure 19: Second Cluster with Pilot as Central Element

The first two clusters are separate from each other because the hazards are influenced by different system elements, but the secondary goal of producing clusters that do not isolate single influences is not met because the first cluster only contains one influence. The relationship between these clusters of hazards and whether or not they should be modified will be discussed in Section 6.4.

The rearrangement process of the hazards and system elements creates a visual clustering effect that appears in the cluster of hazards in Figure 20 containing HA11, HC10, HN10, and HN11. This cluster contains hazards that impact the control and coordination of RPA maneuvers while operating in the civil airspace. The RPA and ATC system elements did not have a high amount of influence on the system as a whole, so these elements were forced to the right side of the matrix. The effect of their location in the matrix results in a set of empty boxes separating the RPA and ATC elements from

pilot, sensor operator, and all other traffic. These empty boxes are not considered a part of the cluster because the elements of radar, data processing unit, and airspace display do not physically influence these hazards at all. Section 6.4 will discuss how the assessor of the IM must analyze these elements since the cluster does cross over them, but at this moment, the empty boxes are considered an artifact of the rearranging process. This cluster is focused on grouping hazards and these hazards are only influenced by the five identified elements.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W	S	W					
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W	S	W					
HA11	RPA is not able to maneuver in time to avoid a potential NMAC	W		W				S	
HC10	Inability to communicate with ATC, resulting in traffic conflict	S	S	W					S
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities	S	W					W	S
HN11	Uncommanded altitude or course deviation that results in a NMAC	S	W	W				S	S
	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly	S	W	W	W	S	W		

Figure 20: Fourth Cluster with Pilot as Central Element

With a cluster of hazards, there is a possibility of including empty boxes that are not just an artifact of the framework visual structure. Figure 20 shows the cluster including two empty boxes for hazard HA11 where the Sensor Operator and Air Traffic Controller do not influence the hazard. The assessor must remember that the objective of the clusters is to maximize the amount of interactions included within the cluster, so bringing together a group of hazards may include some non-influencing elements. The number of non-influencing element can be kept at a minimum, but this may be contradictory. The contradiction requires a balance between an acceptable and unacceptable amount of non-influencing elements to be determined. The system assessor must first consider if there needs to be influence in these boxes or if the hazard should be located in another cluster. The hazard must be compared to the other hazards already included the proposed cluster especially considering the system elements influencing the hazard. If it makes sense that these hazards still be grouped, the non-influencing elements are accepted rather than producing a separate cluster.

Hazard HA11 states that the "RPA is not able to maneuver in time to avoid NMAC." This hazard describes the situation that occurs if an aircraft is detected directly in front of the RPA without previous warning. Previous warning may not occur for

several reasons, but now that the intruding aircraft is detected in front of the RPA, the pilot must attempt to avoid a collision. Depending on the location of the intruding air traffic, the pilot may not deflect the control joystick enough or the RPA may not be able to physically maneuver in time to avoid an NMAC. Assuming all other systems are working properly, the sensor operator or air traffic controller cannot change the physical properties of the RPA or the pilot's ability to control the RPA. Therefore, they do not have influence. The SO and ATC do not have influence into the ability of the aircraft itself. It could be argued, that the SO could have provided more warning if the radar is situated in a location to prevent this situation or the ATC should coordinate the flight path of an aircraft in the close proximity to the RPA. These arguments are true, but better support the hazard of an undetected air traffic intruder. The behavior of the SO and ATC still do not change the physical properties of the RPA or pilot. These empty boxes have been analyzed, and next, the hazard must be determined if it belongs in the cluster

Even with the empty boxes, hazard HA11 belongs in the cluster with the other three hazards in the cluster, HC10, HN10, and HN11, because they are influenced by similar systems and the nature of hazard is similar to the rest of the cluster. The hazards are all influenced by elements that are included in at least three different major system groups. All of the hazards are influenced by the crew, all other air traffic, and either the RPA or ATC. Those system elements are completely unrelated in function and location of system hardware. They are all uninfluenced by the radar data processing major group. The hazard HA11 is similar to that of the other hazards because all of these explain control and coordination of the RPA movements in the airspace.

6.4 Discussion of Clustering Results

After the clustering process was applied to the IM framework using three different central elements, the results were compared to see if the clustering technique produced different clusters of hazards. Beyond discussing the overall results, a detailed comparison of the clusters developed in each of the matrices will be conducted followed with analysis of the how these results can be used to inform safety assessment methods.

The results of the applied clustering technique are shown in Figures 21, 22, and 23 with the different central elements of pilot, RPA, and radar, respectively. The clusters are numbered in order starting at the top row of the matrix moving downward.

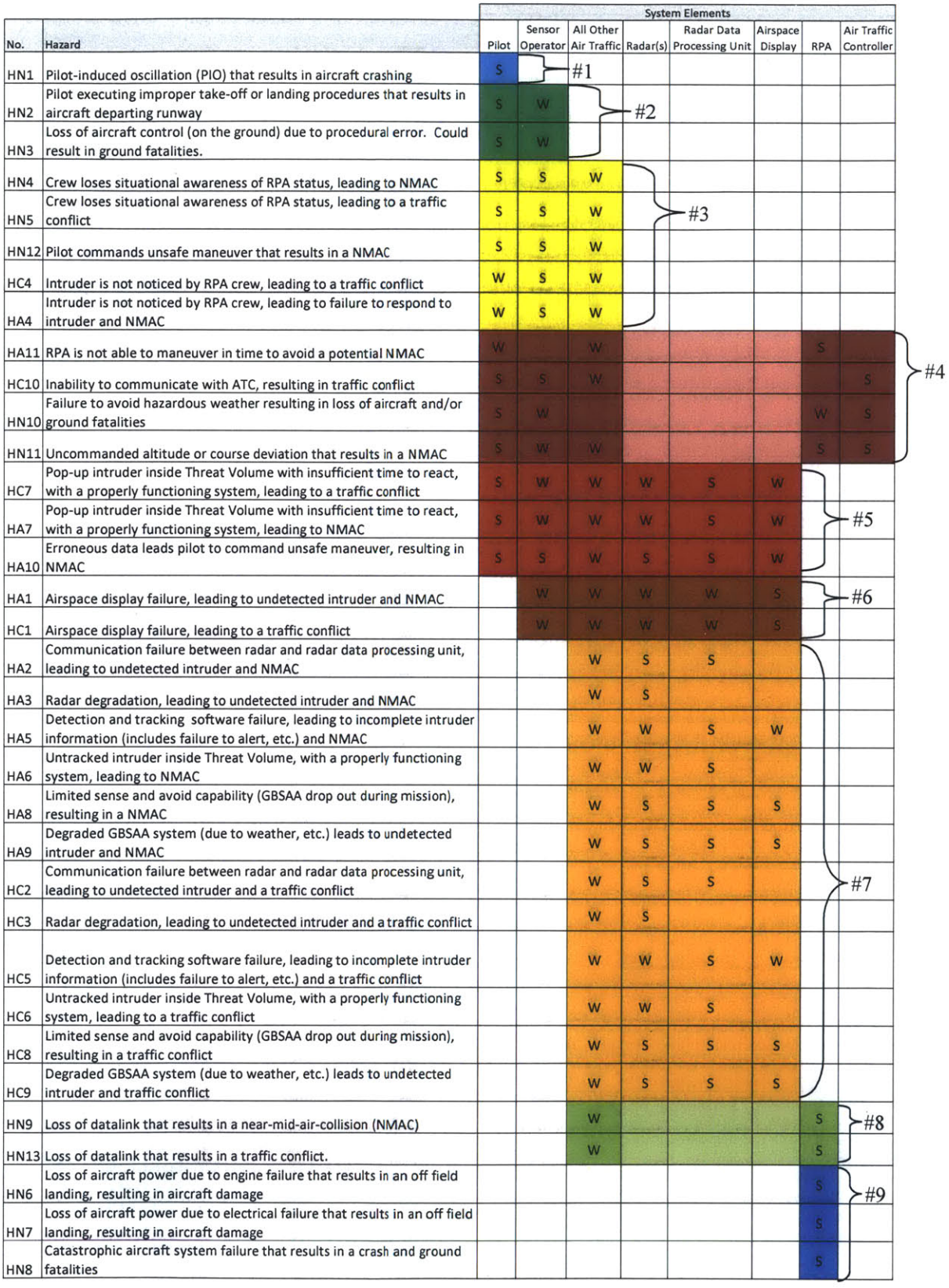


Figure 21: Clusters with Pilot as Central Element

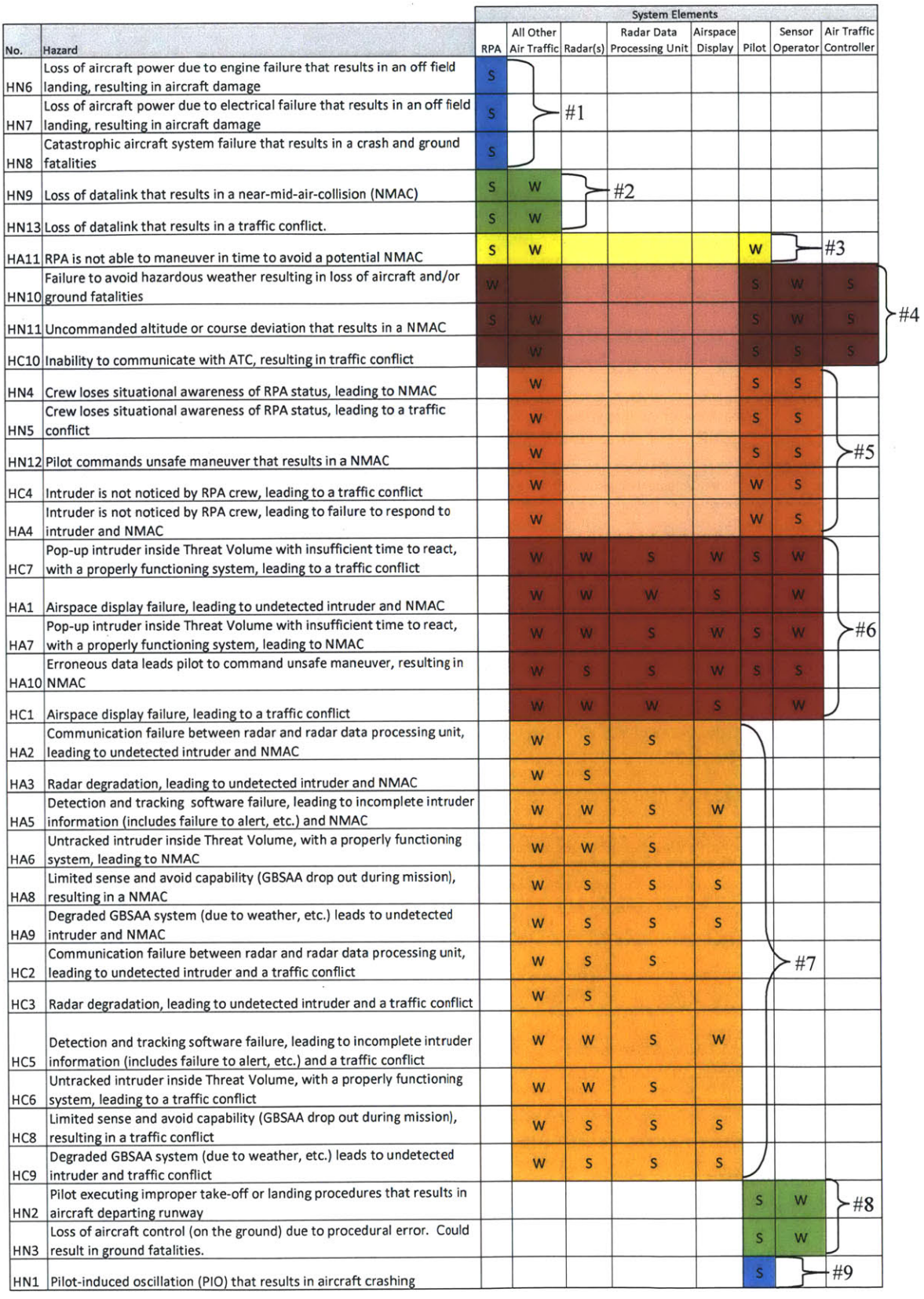


Figure 22: Clusters with RPA as Central Element

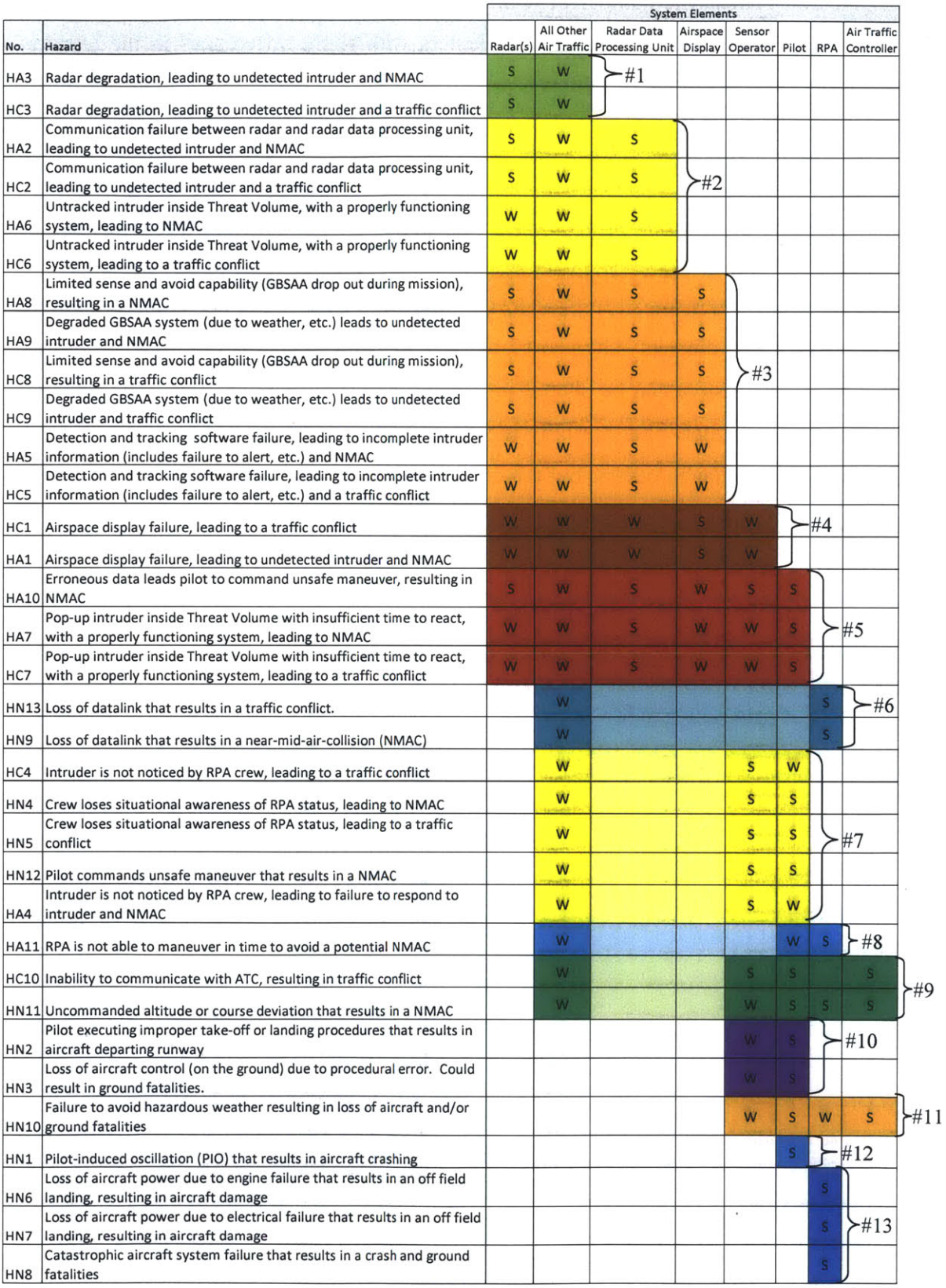


Figure 23: Clusters with Radar as Central Element

At first glance, the number of identified clusters is compared. With the pilot and RPA as a central element, there are nine clusters with slight differences in the hazards included each cluster. When radar is the central element, the technique produced thirteen clusters with even more differences of the hazards included in each cluster when compared to the pilot or RPA results.

Figure 24 is a detailed comparison of the individual identified clusters in each of the central element approaches. The common clusters are identical in each of the approaches. They are identical in the hazards that are clustered and the system elements that influence those clusters. The shared clusters are identical in only two of the three approaches. The clusters can be shared in three different pairs are shown in Figure 26. Unique clusters are those that are only identified in one of the approaches. The unique clusters may be similar to others, but the cluster of hazards and what elements influence that cluster is unique to a specific central element perspective.

Central System: Pilot			
uster #	Hazards within Cluster	# of Influencing Elements	Common, Shared or Unique
1	HN1	1	Common
2	HN2, HN3	2	Common
3	HA4, HC4, HN4, HN5, HN12	3	Common
4	HA11, HC10, HN10, HN11	5	Unique
5	HA7, HC7, HA10	6	Shared with Radar
6	HA1, HC1	5	Shared with Radar
7	HA2, HC2 HA3, HC3 HA5, HC5 HA6, HC6 HA8, HC8 HA8, HC9	4	Shared with RPA
8	HN9, HN13	2	Common
9	HN6, HN7 HN8	1	Common

Central System: RPA			
Cluster #	Hazards within Cluster	# of Influencing Elements	Common, Shared or Unique
1	HN6, HN7 HN8	1	Common
2	HN9, HN13	2	Common
3	HA11	3	Shared with Radar
4	HN10, HN11 HC10	5	Unique
5	HA4, HC4, HN4, HN5, HN12	3	Common
6	HC7, HA1 HA7, HA10, HC1	6	Unique
7	HA2, HC2 HA3, HC3 HA5, HC5 HA6, HC6 HA8, HC8 HA8, HC9	4	Shared with Pilot
8	HN2, HN3	2	Common
9	HN1	1	Common

Central System: Radar			
Cluster #	Hazards within Cluster	# of Influencing Elements	Common, Shared or Unique
1	HA3, HC3	2	Unique
2	HA2, HC2 HA6, HC6	3	Unique
3	HA8, HC8 HA9, HC9 HA5, HC5	4	Unique
4	HA1, HC1	5	Shared with Pilot
5	HA7, HC7 HA10	6	Shared with Pilot
6	HN9, HN13	2	Common
7	HA4, HC4, HN4, HN5, HN12	3	Common
8	HA11	3	Shared with RPA
9	HC10, HN11	5	Unique
10	HN2, HN3	2	Common
11	HN10	4	Unique
12	HN1	1	Common
13	HN6, HN7 HN8	1	Common

Figure 24: Cluster Comparison

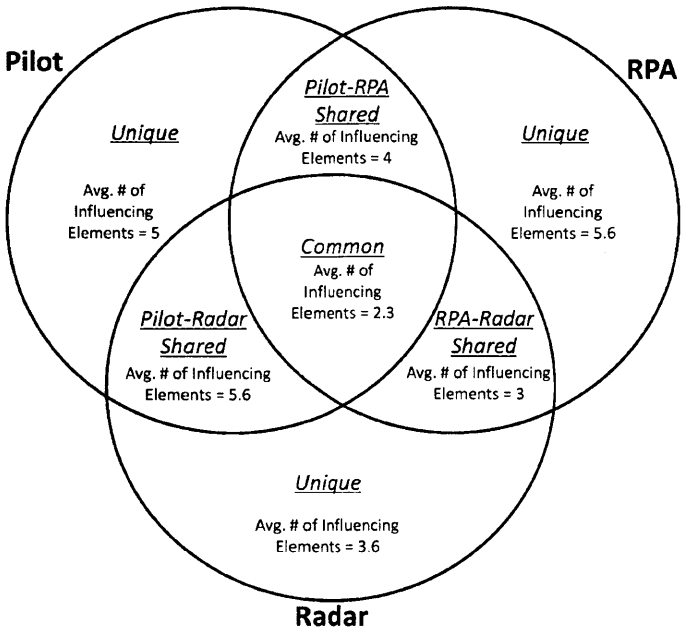


Figure 25: Venn Diagram for Cluster Comparison

The cluster descriptions are shown in the Venn diagram in Figure 25 and the different sections are compared. The common clusters average only 2.3 system elements influencing the clusters. This means that these clusters are influenced by a relatively low number of the elements out of the possible eight. Of the five identified common clusters, the most system elements influencing the cluster was three. None of these clusters where highly influenced by all the elements and because of that, the clusters could be easily separated from the other hazards that are more influenced.

The shared clusters in Figure 25 are to visually distinguish how those hazards are grouped differently depending on the central element. There are some similarities between two of the three approaches. When the pilot is the central element, cluster #5 and #6 were identically identified when the radar is the central element. With the radar as the central element, the corresponding clusters are #5 and #4, respectively. Also, when the pilot is the central element, cluster #7 matched cluster #7 with the RPA as central element. Lastly, when the RPA is the central element, cluster #3 matched cluster #8 for when the radar is the central element.

The insight gained from the shared clusters is that the influences of the system elements are tightly coupled even when focused on different central elements. The different central elements did not break these clusters apart and verifies the identification

of a cluster. Since the hazards are so tightly coupled there is no need to separate these hazards into smaller clusters. The high interaction between the elements and hazards allows the assessor to examine the system in groups rather than each hazard individually.

The unique clusters have the most influencing elements on average when compared to common clusters. The unique clusters have an average of 5, 5.6 and 3.6 influencing elements for the pilot, RPA, and radar approaches respectively. The highly influenced hazards have more possibilities to be included in or separated from clusters that are identified in each matrix. The highly influenced hazards are difficult to differentiate from other hazards because they are influenced by similar system elements of many other hazards.

The insight gained from the unique clusters is the difficulty to differentiate highly influenced hazards from other hazards. The reason for this difficultly is because the highly influenced hazards have similar element behavior impacting the risk of the hazard. A highly influenced hazard may be impacted by six elements including the central element, so the hazards influenced by those same elements could be grouped with this hazard. The unique clusters appear because the central element focus draws those highly influenced hazards towards the elements that behave similarly to the central element.

The unique clusters impact the safety assessment process because the highly influenced hazards will need to be assessed in detail to ensure the adequate mitigation strategies are in place to handle each influence contributing to that particular hazard. The difficulty in differentiation highlights the complexity of the system and requires the attention of system experts to further assess those hazards.

When focused on the different central elements, the results produced a high level of granularity and detailed focus on the central element and those elements behaving similarly to it. An example of this with the radar is the central system is discussed. The first three clusters of hazards that were identified with the radar as the central element are identified as one cluster when the pilot or RPA is the central system. This is intuitive because if the radar is the central system, more attention is placed into rearranging it influences rather than on the pilot or RPA influences. The opposite is true when the other systems are central. When the pilot is the focus, the detailed assessment will be less focused on the radar system. The difference in detailed focus reinforces the need for

multiple experts to be involved in the safety assessment process to provide detail on the entire system rather than on just one central element.

The clusters identified when the radar is the central element are more separated out than the other two methods because increased granularity around the radar functionality. This is why the radar-centered matrix had four more clusters than the other two matrices. The process called for the hazards influenced by the radar data processing group to be separated into three clusters, but those same hazards are only one hazard when the pilot and RPA are the central elements.

The clustering process also required the radar element to be separated from the other elements within its major system group. The all other air traffic element influenced more similar hazards to the radar than the radar data processing unit or the airspace display. This occurred because most hazards created by a radar influence led to an NMAC or traffic conflict which requires the influence of air traffic. If air traffic is not present, the state in which the sensing function is in does not pose a hazard to the overall system.

The effect of external aircraft is consistent with the IM definition of influence using the partial derivative. The behavior of the external aircraft system element resulted in a change in risk of the NMAC hazard. It is not a strong influence because the hazard is strongly created by a fault within another element to allow the external aircraft to get too close to the RPA to create an NMAC situation. The external aircraft is constantly changing its position and with each change in position, the level of risk for an NMAC changes, but not in large magnitudes. It can be argued that the loss of radar functionality is a hazard with or without air traffic because there would be no way to detect future intruding aircraft, but again the hazard only depends on the presence of air traffic. Without other air traffic there would be no need to use a GBSAA system at all.

An insight gained from looking at the "All Other Air Traffic" system element is its relative influence on all hazards compared to other system elements. The "All Other Air Traffic" system element has influence on the highest number of hazards out of all other system elements. This is expected because the main reason GBSAA is being used is to avoid the external aircraft. If no external aircraft operated in the NAS, then there would be no concern for aircraft safety. That is why an RPA can operate in restricted

airspace without a COA because no other aircraft are present in that area. The high number of hazards influenced shows the relative importance of each system element. This relative importance emphasizes that external aircraft must be monitored closely to ensure a traffic conflict and NMAC do not occur. If any system impacts the ability to monitor the external aircraft, a large amount of risk will be incurred.

The more detailed focus on the central system element is reinforced by the Venn diagram in Figure 25. The diagram shows that the common clusters have a lower average number of influencing elements than the unique clusters. The insight gained from the higher average number of influencing elements is that when a different element is used as a frame of reference, how that central element influences those hazards that are also influenced by the majority of other elements changes. With that difference in influence, the way in which the highly influenced hazards are clustered is different because there is more focus placed on the central element rather than the clusters themselves. As an example, the pilot on average uniquely influences more hazards where five elements influence those same hazards. While the radar element on average more uniquely influences hazards in which only three elements influence those same hazards.

The most unique clusters across all three matrices are identified as one cluster for when the pilot is the central element and multiple clusters when the RPA and radar are the central elements. These clusters include hazards HA11, HC10, HN11, and HC10. This cluster is separated into two clusters when the RPA is the central element and three clusters when the radar is the central element. All of these are considered unique clusters when classified in the Venn diagram.

The insight gained from the most unique clusters across all three approaches is that these hazards are influenced by a large number of elements but not so many that each central element behaves the same for each hazard. The different central elements classify these hazards differently because of granularity of focus placed on those systems behaving similar to the central element. The difference in the clusters draws the attention of the assessor to examine these hazards again. This highlights the importance of system experts to examine these hazards closely. The IM is successful in allowing the experts to focus their efforts on only a few of the hazards in question rather having to examine all hazards again.

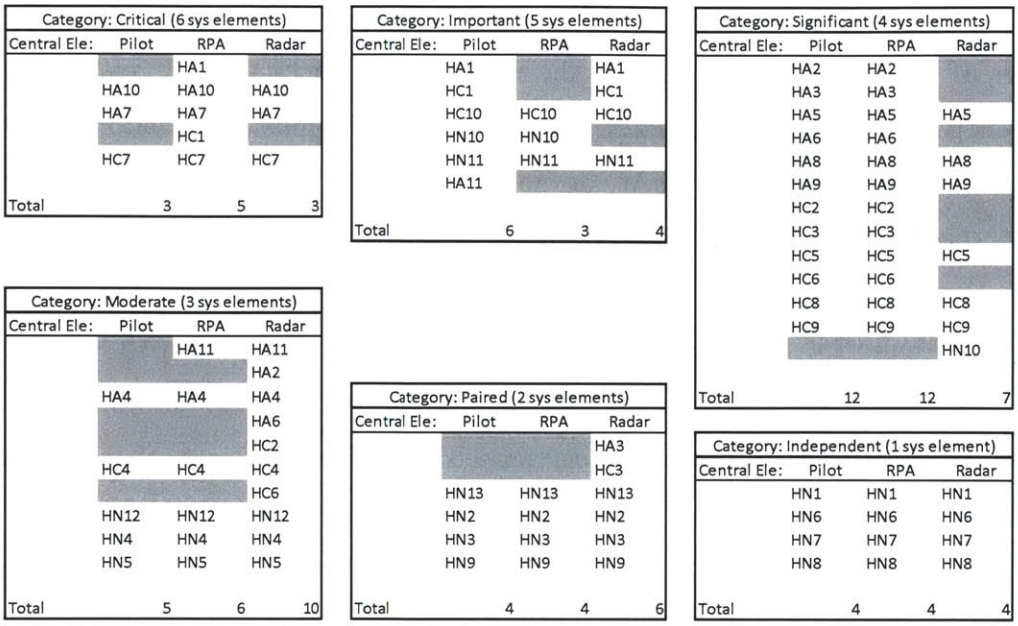


Figure 26: Hazard Comparison by Category

In Figure 26, the individual hazard results of each matrix are compared. The categories for the figure are as follows: Critical clusters have six system elements influencing the cluster, Important have five elements influencing the cluster, significant have four elements, moderate have three, Paired have two, and Independent have one system element influencing the cluster.

Starting with the critical hazards that are highly influenced, all three matrices identified HA10, HA7, and HC7. These three hazards are clear critical hazards since all three matrices produced these results. The RPA focused matrix clusters identified hazards HA1 and HC1 as critical, but the other two matrices identified them as important separating them out because they are only influenced by five elements instead of six. Next, the IM with the pilot as the central element identified more important hazards with multiple system influence than the other two IM's. The IM focused on the pilot and RPA did include more empty boxes than when the radar is the central element. These differences will be discussed further to analyze if one approach is condensing or separating clusters too much.

The insight gained from more hazards identified as important hazards is that the central element may be simplifying hazards too much. This occurs when one hazard has similar element influence to other hazards, but is actually influenced by more elements

that any other hazard it is grouped with. This forces the group to include many empty boxes while elevating the category of the hazards. The IM focused on the pilot and RPA did include more empty boxes than the radar matrix, so that could also expose that simplification of clusters.

The impact that simplification has on safety assessment is that the some system elements will be assessed for more hazards than they actually impact. That extra assessment can be expensive if testing must be conducted, and resources may be taken away from those hazards that need the extra assessment and testing.

Figure 27 depicts three clusters to be used as an example for how the clusters are used to formulate mitigation strategies.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S	W						
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S	W						
HN4	Crew loses situational awareness of RPA status, leading to NMAC	S	S	W					
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict	S	S	W					
HN12	Pilot commands unsafe maneuver that results in a NMAC	S	S	W					
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W	S	W					
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W	S	W					
	RPA is not able to maneuver in time to avoid a	W		W				S	

Figure 27: Three Example Clusters

For the first cluster, the pilot has a hazard of a pilot induced oscillation (PIO). The mitigation strategy needs to address the pilot's ability to recognize and handle a PIO. Since no other element is included in the influence of this hazard, so there is no need to have mitigation strategies in place for the sensor operator or radar. Those outside elements are not simply ignored. The assessor reconsiders the hazard to double check that the outside elements truly do not influence a PIO.

The next cluster from the top, the pilot and SO crew members have a hazard of losing control of the aircraft due to improper procedures on the ground and during landing or take-off. The mitigation strategy needs to address the crew member's training and ability to follow procedures correctly.

For the third cluster, the RPA crew must maintain situational awareness, safe maneuvers of the RPA, and monitor the airspace display as to not end up in an NMAC or traffic conflict situation. The mitigation strategy must address the crew training and the

ability to monitor the external aircraft. The crew can lose situational awareness with no other aircraft present, but the hazard does not become apparent until the external aircraft is close to the RPA. Since the all other air traffic influences the hazards in this cluster, the mitigation strategy must keep the external aircraft away from the RPA at all time. The other part of the mitigation strategy is to ensure the crew has the ability to monitor the airspace.

The clustering technique allows the assessor to handle hazards in groups of similar system elements as well. The mitigation strategies focus only on a few system elements. An example of this is that the air traffic controller does not need to know how to identify and solve a procedural error created by the RPA crew.

Beyond determining mitigation strategies, the IM framework provides an opportunity to condense the safety assessment. Within a particular cluster, there may be repetitive hazards or hazards that may be combined to help condense the safety assessment. Even separate clusters may be combined if the assessor decides the two clusters are to be examined together rather than separately. Again Figure 27 will be used to provide examples.

In the third cluster there are a few repetitive hazards. The hazards of the crew losing situational awareness and not noticing the intruder aircraft are each repeated twice. They are repeated twice because the hazard of an NMAC and traffic conflict differ in severity, but in terms of hazard influence, the system elements behave identically for an NMAC or traffic conflict. As long as the mitigation strategy prevents the crew from losing situational awareness or failing to notice the intruding aircraft then both an NMAC and a traffic conflict can be avoided. Functionally, condensing hazards allows the assessor to focus attention on one hazard rather than having to deal with each hazard individually. The assessor must be careful not to condense the IM too much. Only if the safety behavior of multiple hazards is identical should they be condensed. If the assessor feels condensing the hazards may negatively impact the safety of the system, do not condense.

The first and second clusters involve crew procedure situations that may be able to be joined together into one cluster. The argument of the first hazard cluster is that the SO does not impact a PIO, but the SO may be able to be aware of what a PIO looks like

and could point it out the pilot as it is occurring. If the clusters are combined, the focus of the assessor is again reduced to one cluster rather than two. The mitigation strategies will have to be expanded to train the SO on PIO's. If the joining of two clusters is judged to negatively impact the safety assessment, then the clusters will remain separate.

Further examination of each empty box forces the assessor to think address the idea that the cluster is wrong and needs to be broken down into smaller units to eliminate the empty box. The empty boxes in each cluster expose where the assessor set the threshold for influence because the element is included in the cluster but did not influence the hazard enough to be labeled a weak or strong influence. The assessor needs to double check the empty box to determine if the element actually does have influence on that hazard. This empty box can provide a sanity check for the identification of the clusters.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W	S	W					
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W	S	W					
HA11	RPA is not able to maneuver in time to avoid a potential NMAC	W		W				S	
HC10	Inability to communicate with ATC, resulting in traffic conflict	S	S	W					S
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities	S	W					W	S
HN11	Uncommanded altitude or course deviation that results in a NMAC	S	W	W				S	S
	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly	S	W	W	W	S	W		

Figure 28: Large Example Cluster

In Figure 28, the large cluster at the bottom of the figure will be examined for its empty boxes. The hazard cluster contains hazards that involve the crew dealing with a particular system element failure outside the GCS, but does not involve the radar data processing major group elements. The top hazard, "HN11 – RPA is not able to maneuver in time to avoid a potential NMAC," has three empty boxes to be examined. The first shows no influence from the sensor operator. The SO does not control the RPA, nor does the SO have an impact on the physical abilities of the RPA. Changes in the SO's behavior will not impact the risk of hazard HN11 occurring resulting in an empty box in the matrix. Next, the airspace display does not influence the hazard. Again, the display cannot change the abilities of the pilot or RPA, so the behavior of the display does not impact the risk of hazard HN11 occurring. The last empty box shows the ATC has no influence and again, the behavior of the ATC does not impact the risk of hazard HN11

occurring. This quick inspection of the cluster and empty boxes helps verify the ability of the IM to capture system behavior and hazard influence.

6.5 Summary of Clustering Application

The application of the influence matrix framework and cluster technique produced several interesting detailed results, but those details can be summarized into boarder insights that can be compared to the traditional safety assessment methods. These board insights help extend the knowledge for safety assessment methods and provide rationale why the IM is an innovative way to assess system safety.

An advantage of the IM framework is the visual link between system elements and hazards. The direct visual connections allow the assessor to understand which system elements impact system hazards. The overall number of influences populating the matrix shows the assessor how complex and tightly coupled the system as a whole.

In contrast to the IM, the FTA and FHA methods can grow in exponential fashions and be difficult to understand. It is difficult to quickly assess and determine which system element impacts the largest number of hazards by visual examination of an FTA or FHA. As the assessors decompose a system into more detail, the FTA adds a new layer that is usually more numerous than the layer before, and the FHA adds new functions and systems to the list. There is no direct connection to the hazards themselves in either method. The FHA points to functions which can be mapped to hazards, but the final IM illustrates that direct connection without having to reason through all the functions first.

A second broad insight gained from the application of the IM is the flexibility of the matrix format. The matrix format allows the assessor to rearrange and manipulate the order of the hazards and system elements to draw conclusions about the system behavior. The clustering technique takes advantage of the flexibility of format. The clustering process of rearrangement and cluster identification functions to constantly reevaluate and examine the hazards and influencing elements. This technique ensured the IM framework produced an accurate description and model of the overall system.

The flexibility of the format is a major advantage of this method for initial assessment of complex systems. The flexible format is capable of handling large lists of

system elements and large lists of hazards. Even the way the influences are defined is flexible. The influences can be binary values or even quantified numbers. The assessor of each system while have to choose what qualities of the matrix will be best on a case-by-case basis. It may not be possible to force a rigid safety assessment process upon a newly complex system, so the flexible matrix format can be adjusted to better assess the safety of the new system.

Unlike the IM, the FTA and FHA are rigid safety assessment methods. The FTA and FHA cannot switch around branches or subsystems because it would lose the structure of the method. The structure of the method helps the assessor separate independent elements or activities, but with a complex system like GBSAA, there are no completely independent system elements. The specific FTA and FHA structure can make it difficult for a user to follow the information provided or find the answer to a specific question relating to hazards. The IM condenses more information in a smaller area than the FTA or FHA. This provides the opportunity for a complex system to be defined in one or two pages rather than ten or more pages.

A structured FTA calls for each branch to be independent of each other, but as systems continue to become more complex, it is difficult to find elements that do not have a relationship with multiple other elements. The high amount of system influences makes it difficult to create an FTA that only lists a particular system hazard in one branch. One hazard may be influenced by several conditions which relate to other hazards. For the example used at Cannon AFB, the information and functions operate in a loop form. The pilot talks to the RPA which is detected by the radar that sends information to the data processor to display in the GCS to the pilot how makes a decision on what to send back to the RPA. Any function in that loop is influenced by all the elements within the loop. No one system is completely independent.

The third broad insight gained is the ability of the identified clusters to provide the assessor with a priority of hazards and system elements. The clusters identify the specific elements that similarly behave or influence hazards and the overall system safety. The grouping of common system behavior and influenced hazards provides the assessor with an understanding of which hazards are critical and which system elements are tightly coupled to those hazards. That understanding provides a basis for mitigation

strategies to be better formulated to prevent single or multiple hazards. This priority system can also be used to help plan a limited testing schedule or allocate finite resources towards a particular hazard mitigation or system element.

The fourth broad insight emphasizes the importance of evaluating as system from multiple perspectives. The clustering results explained the detailed differences between the identified clusters within the central element approaches. Beginning each clustering process with different central elements increased granularity and detailed attention on that element but abstracted out those hazards and elements not closely linked to the central element. This highlights the importance of assessing the safety behavior of an entire system with the perspective of multiple elements of focus. It is important for an expert on radar to focus on how the aircraft influences hazards rather than just explain the radar's impact on hazards. It is also important to begin each safety assessment at different points of the system rather than always using one standard approach. The different cluster results exposed that importance that evaluating the system from multiple perspectives will ensure the detailed influences will be explained from all angles.

The IM framework is a detailed assessment method for modeling system architecture elements and their relationships. While clustering in this thesis was visually motivated, several objectives were identified to standardize the process. Simply building the IM encourages several people and teams of experts to increase their understanding of the system. That knowledge is important for safety assessment because with more information understood about the behavior of the system the assessor can better plan to prevent hazards.

Chapter 7

Conclusions and Future Research

Remotely piloted aircraft operations in the National Airspace System require a safety assessment process that is reviewed by the Federal Aviation Administration as a part of the Certificate of Authorization application. An approach was taken in this thesis to analyze the application and evaluation a set of traditional safety assessment processes used by the Air Force Safety Center for military RPA operations at Cannon AFB using a Ground-Based Sense and Avoid system.

The research completed for the Air Force Safety Center's Risk Management document provided experience with the safety assessment process, a formal list of hazards for the GBSAA system, architecture diagram, FHA and FTA. That information was leveraged to apply as a case study of the influence matrix framework. The case study was motivated by scoping challenges identified in the use of traditional methods and by previous research outlining the need to apply a formal clustering approach. The clustering technique provided an opportunity to group hazards and address challenges in the scope of the safety assessment. In turn, this would allow resources to be better allocated towards designing mitigation and control strategies in the complex system.

Several insights were gained from the IM framework case study in reference to the actual framework model, applied clustering technique, clustering results, and comparisons to the FTA and FHA. The IM framework was shown to provide a visual link between system elements and hazards. The direct visual connections allowed the assessor to understand which system elements impact system hazards which contrasted the large and difficult to understand FTA and FHA methods. Next, the IM illustrated flexibility to rearrange and manipulate the order of the hazards and system elements to draw conclusions about the system behavior and ensured an accurate description of the overall system. Then, the IM revealed the advantage of identified clusters providing the assessor with a priority of hazards and importance of system elements. Finally, the case study highlighted the importance of evaluating as system from multiple perspectives. It

was important to begin the safety assessment at different points of the system rather than always using one standard approach. The different starting points provide the system with a detailed assessment of all hazards and not those just evaluated with one central perspective leaving some elements and hazards abstracted out and generally grouped together.

Although valuable insights were gained, some aspects of the IM can be explored further for future research. In applying clustering techniques, some subjectivity was apparent in how to group system elements and hazards. If clustering was confined to a standard mathematical algorithm, the results may be more consistent no matter what element is chosen as a central element. Research could be conducted to build a mathematical algorithm, but more values for defining influence rather than just strong, weak, or no influence may need to be defined or quantified.

In this case study, the IM was not used to create numerical values for risk or overall influence values. The FTA uses functions associated with an "or" or "and" statement in the structure, but the IM does not have a strict mathematical function associated with the influence boxes in the matrix. The influence is more of a judgment by the assessor using the input of system experts. Future research can explore if there is a method that can be applied to the matrix to provide an actual quantitative value for how much risk is increased or decreased by a system element.

Future research can be applied to a formal approach to condense and streamline the safety assessment method. This condensing method could be formulated so that future, more complex systems can be understood in simple terms. Future research may be forced to focus greater detail in defining a level of interaction between systems. Simply managing those interactions will be important so that risks can be mitigated and system testing can be easily managed.

A drawback of the IM is the fact that this method is not well established or tested. The framework needs the FTA and FHA to help verify correct information, but currently, the IM framework is not trusted enough for use. System experts must conduct separate research to see if the IM framework performs as expected or provides useful results. Comparing the IM to existing traditional methods helps promote creditability for the IM.

The review of clustering techniques applied to DSMs identified using a tearing approach that could possibly be used with the IM. When a system element seems to complicate the model, it could be possible to "tear" away that element and assess the new results and see what changed [35]. This may even help provide better results for this IM because it will increase detailed assessment of less system elements. The tearing method was not applied to this case study, but future work could explore this approach.

The last identified area for future research is examine the IM's ability to respond to change within the system quickly after it has already been defined by the IM method. If a system element changes its inputs or outputs, the relationships between the hazards and other system elements may change. The entire matrix may have to be re-evaluated with each change.

In closing, The IM framework was a detailed assessment method for modeling system architecture elements and their relationships to hazards. Building the IM had one major benefit above all other insights. That benefit was the increased understanding of the GBSAA system and safety assessment process for future complex systems. That knowledge is important because with more information understood about the behavior of the systems, better plans can be formulated to prevent hazards.

(this page intentionally left blank)

Appendix A

List of GBSAA Hazards Resulting in NMAC (Near Mid-Air Collision) [2]

#	Hazard List
HA1	Airspace display failure, leading to undetected intruder and NMAC
HA2	Communication failure between radar and airspace processor, leading to undetected intruder and NMAC
HA3	Radar degradation, leading to undetected intruder and NMAC
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC
HA5	Software failure, leading to incomplete intruder information (includes failure to alert, etc.) and NMAC
HA6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to NMAC
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC
HA8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a NMAC
HA9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and NMAC
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC
HA11	RPA is not able to maneuver in time to avoid a potential NMAC

List of GBSAA Hazards Resulting in Air Traffic Conflict (but not NMAC) [2]
Traffic within 5 nm horizontally and 1000 feet vertically

#	Hazard List
HC1	Airspace display failure, leading to a traffic conflict
HC2	Communication failure between radar and airspace processor, leading to undetected intruder and a traffic conflict
HC3	Radar degradation, leading to undetected intruder and a traffic conflict
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict
HC5	Software failure, leading to incomplete intruder information (includes failure to alert, etc.) and a traffic conflict
HC6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to a traffic conflict

#	Hazard List
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict
HC8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a traffic conflict
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict
HC10	Inability to communicate with ATC, resulting in traffic conflict

List of RPA Hazards Not Related to GBSAA [2]

#	Hazard List
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.
HN4	Crew loses situational awareness of RPA status, leading to NMAC
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict
HN6	Loss of aircraft power due to engine failure that results in an off field landing, resulting in aircraft damage
HN7	Loss of aircraft power due to electrical failure that results in an off field landing, resulting in aircraft damage
HN8	Catastrophic aircraft system failure that results in a crash and ground fatalities
HN9	Loss of datalink that results in a near-mid-air-collision (NMAC)
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities
HN11	Uncommanded altitude or course deviation that results in a NMAC
HN12	Pilot commands unsafe maneuver that results in a NMAC
HN13	Loss of datalink that results in a traffic conflict.

Appendix B

Functional Hazard Analysis [2]

SYSTEM	FUNCTIONAL DESCRIPTION	HAZARD/FAILURE CONDITION
1.0 Ground-Based Sensors	• Detect[1] and track[7] any objects within field of view of the sensors • Transmit sensor data to processing units	---
1.1 Radar	• Detect[1] any objects within field of view	• Fails to detect[1] (hardware failure, algorithm failure, normal non-detection)
		• Perform falsely (detect[1] non-aircraft, inaccurate plot[2])
	• Transmit sensor data to Radar Data Processing Unit	• Fails to perform (hardware or software failure, lost connection)
		• Perform incorrectly[4] (incomplete or corrupt data sent)
1.2 Radar Data Processing Unit	• Receive and process data from radar(s)	• Fails to perform (hardware or software failure, algorithm failure)
		• Perform incorrectly[4] (incorrect format, corrupt data)
	• Initiate and maintain tracks[7] of aircraft	• Fails to perform (hardware or software failure, algorithm failure)
		• Perform incorrectly[4] (inaccurate track[3])
	• Transmit compiled data to Airspace Display	• Fails to perform (hardware failure, lost connection)
		• Perform incorrectly[4] (incorrect or corrupt data sent)
2.0 Ground Control Station	• Provide command and control of the RPA • Provide situational capability for RPA in launch and mission phases	---
2.1 Airspace Display	• Provide pilot and sensor operator with sensor information describing the local airspace	• Fails to perform (No data received from processor, software or hardware failure to display data)
		• Perform incorrectly[4] (data not displayed correctly, improper screen settings)
	• Provide both visual and audio alerting to pilot and sensor operator	• Fails to perform (software or hardware failure to alert, speaker failure, screen failure)
		• Perform falsely (alerts goes off unnecessarily)
2.2 Sensor Operator	• Maintain situational awareness of airspace	• Fails to perform (does not look at display)
		• Perform incorrectly[4] (interprets display incorrectly or misunderstands pilot)
2.3 Pilot	• Control of RPA through pilot interface/datalink	• Fails to perform (hardware or software failure, loss of link[5])
		• Perform incorrectly[4] (unintentionally maneuver aircraft)

SYSTEM	FUNCTIONAL DESCRIPTION	HAZARD/FAILURE CONDITION
	• Maintain situational awareness of airspace/RPA	• Fails to perform (loss of communication with ATC, or does not look at display)
		• Perform incorrectly[4] (interprets display incorrectly or misunderstands ATC or sensor operator)
	• Respond to traffic changes in airspace	• Fails to perform (does not maneuver aircraft when necessary)
		• Perform incorrectly[4] (maneuvers in wrong direction)
3.0 Remotely Piloted Aircraft (RPA)	• Maintain flight in airspace as directed by the pilot	• Fails to perform (loss of link[5], subsystem failure of power, controls, etc)
		• Perform incorrectly[4] (aircraft maneuvers without pilot input: wind, software error, improper procedures, etc)
4.0 All Other Air Traffic	• Fly in correct airspace • Fly under proper flight rules and regulations	---
4.1 Cooperative (IFR) Air Traffic	• Fly in correct airspace	• Fails to perform (aircraft enters restricted airspace without authority)
		• Perform incorrectly[4] (aircraft misunderstands ATC instructions)
	• Fly under proper flight rules and regulations	• Fails to perform (aircraft flying too fast, too low, etc without authority)
4.2 Non-cooperative (VFR) Air Traffic	• Fly in correct airspace	• Fails to perform (aircraft enters restricted airspace without authority)
	• Fly under proper flight rules and regulations	• Fails to perform (aircraft flying too fast, too low, etc without authority)
5.0 Air Traffic Control	• Monitor local airspace around Cannon AFB • Ensure FAA rules and regulations are being followed • Coordinate maneuvers with air traffic in local area	---
5.1 Airspace Display	• Provide controller with sensor information describing the local airspace	• Fails to perform (No data received from sensors, software or hardware failure to display data)
		• Perform incorrectly[4] (data not displayed correctly, improper screen settings)
5.2 Air Traffic Controller	• Monitor local airspace and airspace display(s)	• Fails to perform (hardware failure, not look at displays)
		• Perform incorrectly[4] (interprets display incorrectly or incorrect mental model of aircraft in airspace)
	• Coordinate maneuvers with air traffic and pilot	• Fails to perform (loss of communication with pilot)
		• Perform incorrectly[4] (misunderstands pilot)

SYSTEM	FUNCTIONAL DESCRIPTION	HAZARD/FAILURE CONDITION
6.0 Back-up Uninterruptable Power Supply (UPS)	• Provide uninterrupted power to critical systems when commercial power fails and generators are not yet operating	---
6.1 Radar UPS	• Provide uninterrupted power to radar when commercial power fails and generators are not yet operating	• Fails to perform (provide no power when needed, batteries dead)
6.2 Airspace Display UPS	• Provide uninterrupted power to Airspace Display Processor when commercial power fails and generators are not yet operating	• Fails to perform (provide no power when needed, batteries dead)
6.3 GCS UPS	• Provide uninterrupted power to GSC when commercial power fails and generators are not yet operating	• Fails to perform (provide no power when needed, batteries dead)
6.4 RPA UPS	• Provide uninterrupted power to RPA when engine power fails and generators are not yet operating	• Fails to perform (provide no power when needed, batteries dead)
6.5 ATC UPS	• Provide uninterrupted power to ATC when commercial power fails and generators are not yet operating	• Fails to perform (provide no power when needed, batteries dead)

Glossary

[1]**Detect** - locate one target at one point in time

[2]**Inaccurate Plot** - all plots data have position errors. Accurate plots have small errors, and inaccurate plots have larger errors. Determining a dividing line between accurate and inaccurate plots/tracks can be difficult. There are marginal cases where a plot with significant error is still helpful to the track process. Analysts must determine the dividing line between accurate and inaccurate.

[3]**Inaccurate Track** - every track has position, altitude, and velocity errors. Some of these are driven by plot position errors, some by timing errors, and some by computer hiccups. Drawing a firm distinction between accurate and inaccurate tracks is difficult. Similar to plots, analysts must determine the dividing line between accurate and inaccurate.

[4]**Incorrectly** - means the system attempted to perform an action but the desired result did not occur

[5]**Lost Link** – The RPA has two potential data links between the Ground Control Station (GCS) and the aircraft. The beyond line of sight (BLOS) link uses SATCOM. There is also a line-of-sight (LOS) link for ops near the local area. If link is lost, the aircraft autonomously maneuvers to its programmed lost link route.

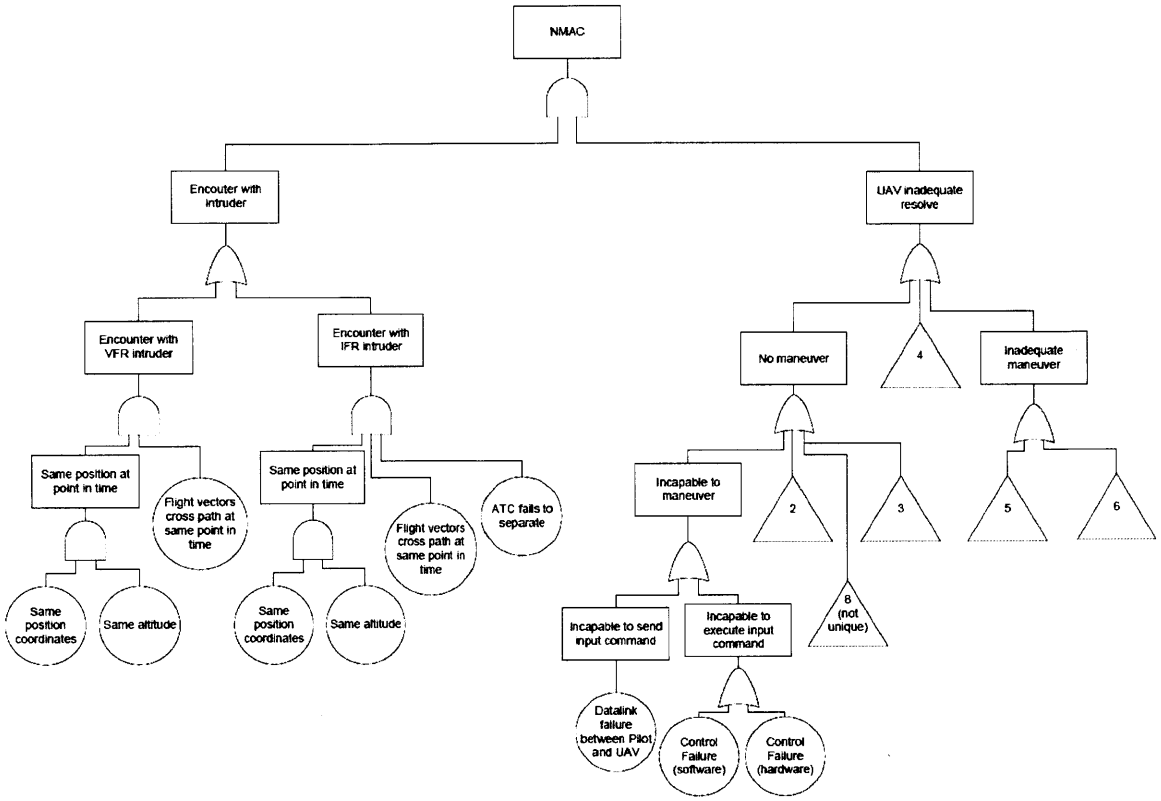
[6]**Plot** - a detection; location (possibly including altitude) of a target at one point in time

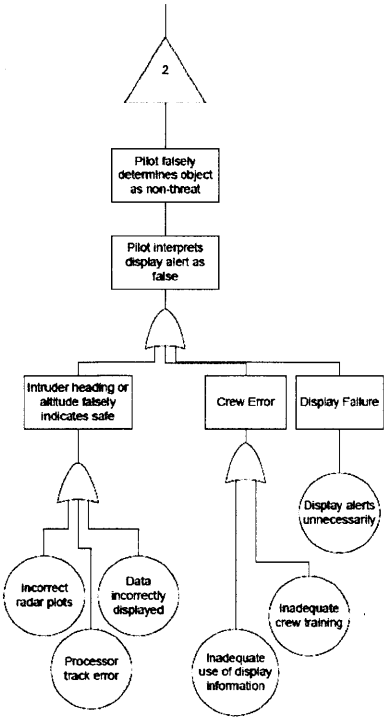
[7]**Track** - a data file (and associated on-screen symbol) representing an aircraft's position, altitude, heading, speed, and possibly other info. A track is initiated from a series of plots that represent the same aircraft over time. It is maintained as long as sufficient plots are reported

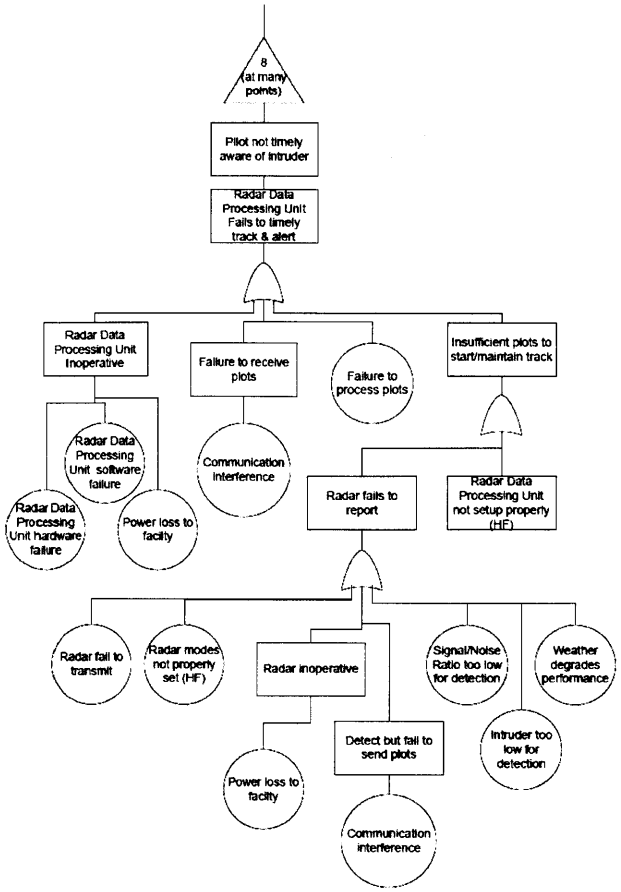
(this page intentionally left blank)

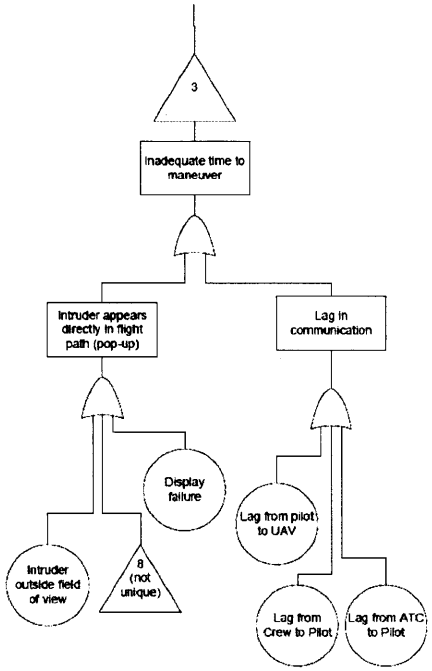
Appendix C

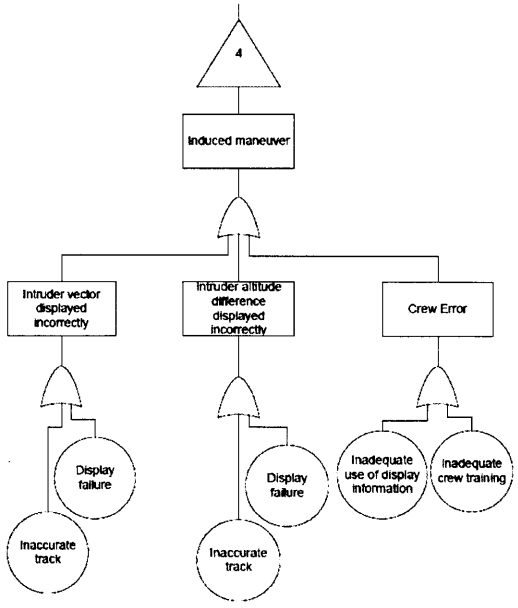
Fault Tree Analysis [2]

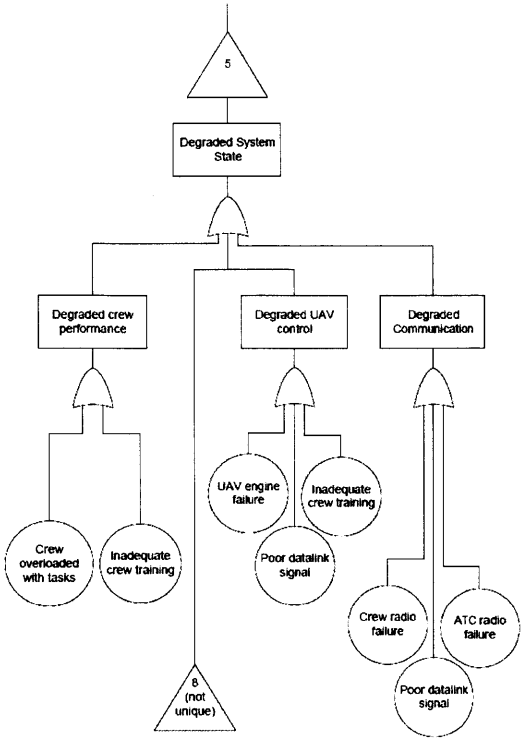


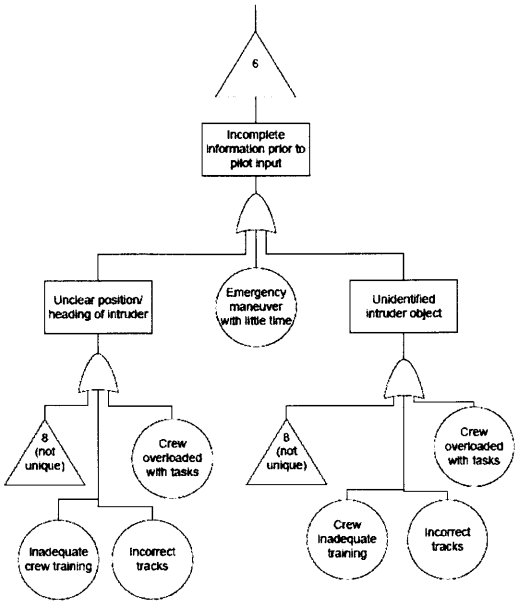

2
Pilot falsely determines object as non-threat
Pilot interprets display alert as false
Intruder heading or altitude falsely indicates safe
Crew Error
Display Failure
Incorrect radar plots
Data incorrectly displayed
Processor track error
Inadequate use of display information
Inadequate crew training
Display alerts unnecessarily


8 (at many points)
Pilot not timely aware of intruder
Radar Data Processing Unit Fails to timely track & alert
Radar Data Processing Unit Inoperative
Failure to receive plots
Failure to process plots
Insufficient plots to start/maintain track
Radar Data Processing Unit software failure
Radar Data Processing Unit hardware failure
Power loss to facility
Communication interference
Radar fails to report
Radar Data Processing Unit not setup properly (HF)
Radar fail to transmit
Radar modes not properly set (HF)
Radar inoperative
Signal/Noise Ratio too low for detection
Weather degrades performance
Power loss to facility
Detect but fail to send plots
Intruder too low for detection
Communication interference


3
Inadequate time to maneuver
Intruder appears directly in flight path (pop-up)
Lag in communication
Display failure
Intruder outside field of view
8 (not unique)
Lag from pilot to UAV
Lag from Crew to Pilot
Lag from ATC to Pilot


4
Induced maneuver
Intruder vector displayed incorrectly
Intruder altitude difference displayed incorrectly
Crew Error
Display failure
Inaccurate track
Display failure
Inaccurate track
Inadequate use of display information
Inadequate crew training


5
Degraded System State
Degraded crew performance
Degraded UAV control
Degraded Communication
Crew overloaded with tasks
Inadequate crew training
UAV engine failure
Inadequate crew training
Poor datalink signal
Crew radio failure
ATC radio failure
Poor datalink signal
8 (not unique)

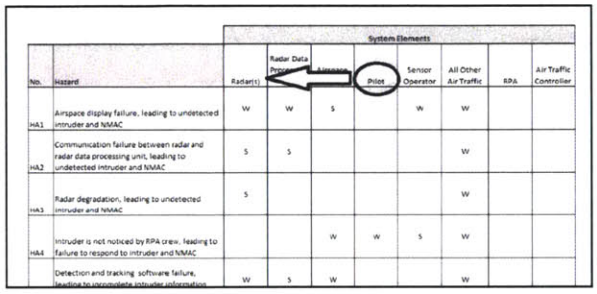

6
Incomplete information prior to pilot input
Unclear position/ heading of intruder
Emergency maneuver with little time
Unidentified intruder object
8 (not unique)
Crew overloaded with tasks
Inadequate crew training
Incorrect tracks
8 (not unique)
Crew overloaded with tasks
Crew inadequate training
Incorrect tracks

(this page intentionally left blank)

Appendix D

Clustering Technique: Step-by-Step Example

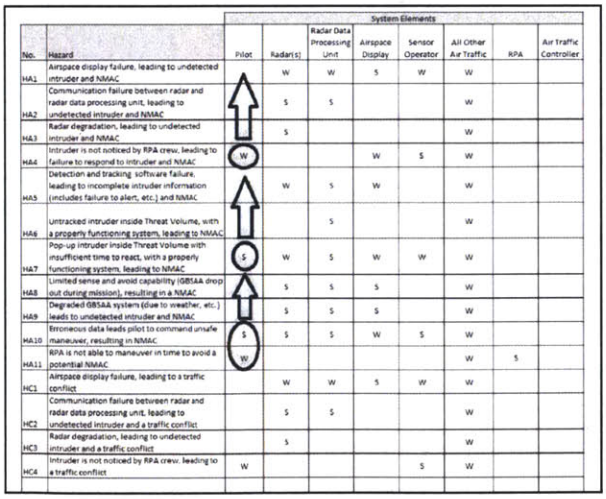
For the clustering process to be explained step-by-step, the pilot will be used as the central element for all pictures as a reference and example. The first step in the process is to begin by reordering the system elements so the central element (with all its influences) is in the farthest left column.



		System Elements							
No.	Hazard	Radar(s)	Radar Data Processing Unit	Airspace Display	Pilot	Sensor Operator	All Other Air Traffic	RPA	Air Traffic Controller
HA1	Airspace display failure, leading to undetected intruder and NMAC	W	W	S		W	W		
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC	S	S				W		
HA3	Radar degradation, leading to undetected intruder and NMAC	S					W		
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC			W	W	S	W		
	Detection and tracking software failure, leading to incomplete intruder information	W	S	W			W		

Step 1

The second step is to rearrange the hazards the central element influences by bringing them to the top of the matrix. Once brought to the top, the hazards will be arranged so the hazard that is influenced by the least amount of other systems should be placed at the top of the matrix. For the pilot example, the hazard located at the top is only influenced by the pilot. The next hazards should be arranged from the least to greatest number of other system elements influencing that hazard.



		System Elements							
No.	Hazard	Pilot	Radar(s)	Radar Data Processing Unit	Airspace Display	Sensor Operator	All Other Air Traffic	RPA	Air Traffic Controller
HA1	Airspace display failure, leading to undetected intruder and NMAC		W	W	S	W	W		
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC		S	S			W		
HA3	Radar degradation, leading to undetected intruder and NMAC		S				W		
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W			W	S	W		
HA5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and NMAC		W	S	W		W		
HA6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to NMAC			S			W		
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	S	W	S	W	W	W		
HA8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a NMAC		S	S	S		W		
HA9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and NMAC		S	S	S		W		
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	S	W	S	W		
HA11	RPA is not able to maneuver in time to avoid a potential NMAC	W					W	S	
HC1	Airspace display failure, leading to a traffic conflict		W	W	S	W	W		
HC2	Communication failure between radar and radar data processing unit, leading to undetected intruder and a traffic conflict		S	S			W		
HC3	Radar degradation, leading to undetected intruder and a traffic conflict		S				W		
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W				S	W		

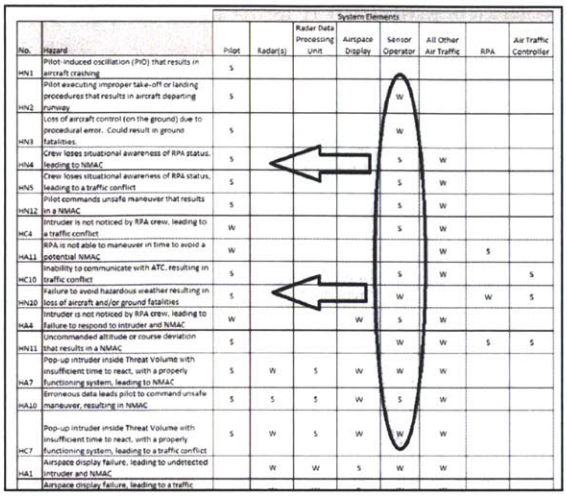
Step 2

The reason for ordering the hazards so that are influenced by the least number of elements are located at the top of the selection and the hazards influenced by the highest number of elements are at the bottom is to centralize the highly influenced hazards. The least influenced hazards at the top will only include the central element and maybe one other element. The more influenced hazards will include more elements which is beneficial for the next step in rearranging. This priority method also brings more influenced hazards up from the bottom of the IM which will help further centralize the most influenced hazards in the center of the IM and the least influenced hazards will be pushed to the top and bottom of the IM.

		System Elements							
No.	Hazard	Pilot	Radar(s)	Radar Data Processing Unit	Airspace Display	Sensor Operator	All Other Air Traffic	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S				W			
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S				W			
HN4	Crew loses situational awareness of RPA status, leading to NMAC	S				S	W		
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict	S				S	W		
HN12	Pilot commands unsafe maneuver that results in a NMAC	S				S	W		
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W				S	W		
HA11	RPA is not able to maneuver in time to avoid a potential NMAC	W					W	S	
HC10	Inability to communicate with ATC, resulting in traffic conflict	S				S	W		S
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities	S				W		W	S
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W			W	S	W		
HN11	Uncommanded altitude or course deviation that results in a NMAC	S				W	W	S	S
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	S	W	S	W	W	W		
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	S	W	S	W		
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	S	W	S	W	W	W		
HA1	Airspace display failure, leading to undetected intruder and NMAC		W	W	S	W	W		
	Airspace display failure, leading to a traffic								

Step 2 Ordering

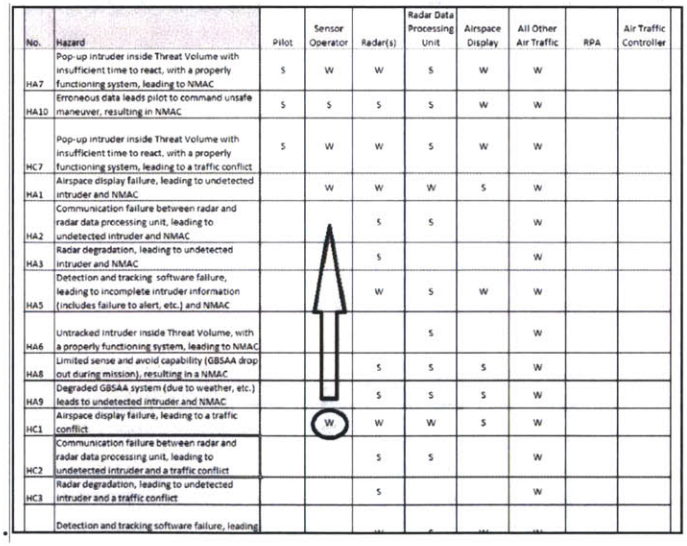
The third step is to look across the rows of matrix at only those hazards the central element influences and determine the system element that influences the highest number of those hazards. In this situation, the sensor operator influences the highest number of those hazards the pilot influences. This described the system element that behaves the most similar to the central element. This example is consistent with the architecture diagram since the sensor operator and pilot have similar functions within the GCS. Once that element is determined, move the element column over to the left side of the matrix situated next to the central element.



No.	Hazard	System Elements: Pilot	Radar(s)	Radar Data Processing Unit	Airspace Display	Sensor Operator	All Other Air Traffic	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S				W			
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S				W			
HN4	Crew loses situational awareness of RPA status, leading to NMAC	S				S	W		
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict	S				S	W		
HN12	Pilot commands unsafe maneuver that results in a NMAC	S				S	W		
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W				S	W		
HA11	RPA is not able to maneuver in time to avoid a potential NMAC	W					W	S	
HC10	Inability to communicate with ATC, resulting in traffic conflict	S				S	W		S
HN20	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities	S				W		W	S
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W			W	S	W		
HN11	Uncommanded altitude or course deviation that results in a NMAC	S				W	W	S	S
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	S	W	S	W	W	W		
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	S	W	S	W		
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	S	W	S	W	W	W		
HA1	Airspace display failure, leading to undetected intruder and NMAC		W	W	S	W	W		
	Airspace display failure, leading to a traffic								

Step 3

The fourth step is to rearrange the hazards again. Those hazards already arranged for the pilot influence should not be adjusted again. Rearrange any hazards influenced by new element (the senor operator in this example) but not influenced by the central element (pilot) by moving them upward to join the group of already collected hazards. Again, do not rearrange any hazards in the upper portion of the matrix that were arranged and prioritized in previous steps.

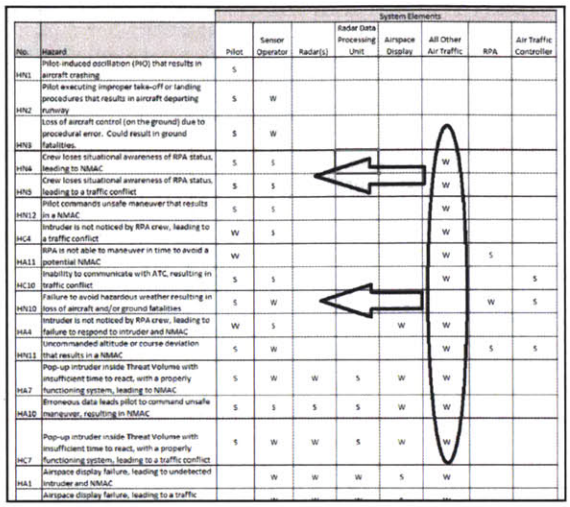


No.	Hazard	Pilot	Sensor Operator	Radar(s)	Radar Data Processing Unit	Airspace Display	All Other Air Traffic	RPA	Air Traffic Controller
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	S	W	W	S	W	W		
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	S	S	W	W		
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	S	W	W	S	W	W		
HA1	Airspace display failure, leading to undetected intruder and NMAC		W	W	W	S	W		
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC			S	S		W		
HA3	Radar degradation, leading to undetected intruder and NMAC			S			W		
HA5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and NMAC			W	S	W	W		
HA6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to NMAC				S		W		
HA8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a NMAC			S	S	S	W		
HA9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and NMAC			S	S	S	W		
HC1	Airspace display failure, leading to a traffic conflict		W	W	W	S	W		
HC2	Communication failure between radar and radar data processing unit, leading to undetected intruder and a traffic conflict			S	S		W		
HC3	Radar degradation, leading to undetected intruder and a traffic conflict			S			W		
	Detection and tracking software failure, leading								

Step 4

This process of moving system elements to the left and hazards upward is repeated until all the hazards and system elements have been moved to their correct position. The fifth step is again to access across rows at only those hazards the pilot and sensor operator influence and determine what other system element influences the highest

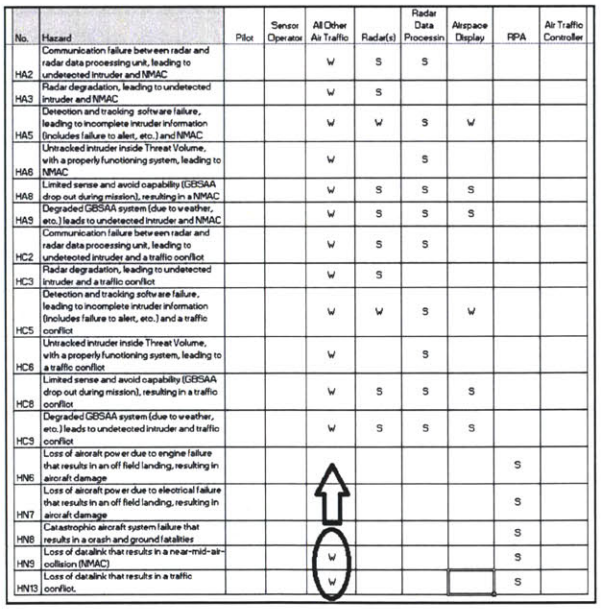
number of those hazards. In this situation it is all other traffic. Now move that element left so it is situated just to the right of the sensor operator column.



		System Elements							
No.	Hazard	Pilot	Sensor Operator	Radar(s)	Radar Data Processing Unit	Airspace Display	All Other Air Traffic	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S	W						
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S	W						
HN4	Crew loses situational awareness of RPA status, leading to NMAC	S	S				W		
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict	S	S				W		
HN12	Pilot commands unsafe maneuver that results in a NMAC	S	S				W		
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W	S				W		
HA11	RPA is not able to maneuver in time to avoid a potential NMAC	W					W	S	
HC10	Inability to communicate with ATC, resulting in traffic conflict	S	S				W		S
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities	S	W					W	S
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W	S			W	W		
HN11	Uncommanded altitude or course deviation that results in a NMAC	S	W				W	S	S
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	S	W	W	S	W	W		
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	S	S	W	W		
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	S	W	W	S	W	W		
HA1	Airspace display failure, leading to undetected intruder and NMAC		W	W	W	S	W		
	Airspace display failure, leading to a traffic								

Step 5

The next step again rearranges the hazards not influenced by the pilot or sensor operator, but are influenced by all other traffic. Rearrange by moving the hazards upward to join the group of already collected hazards. Do not rearrange any hazards in the upper portion of the matrix that were arranged and prioritized in previous steps.



No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processin	Airspace Display	RPA	Air Traffic Controller
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC			W	S	S			
HA3	Radar degradation, leading to undetected intruder and NMAC			W	S				
HA5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and NMAC			W	W	S	W		
HA6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to NMAC			W		S			
HA8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a NMAC			W	S	S	S		
HA9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and NMAC			W	S	S	S		
HC2	Communication failure between radar and radar data processing unit, leading to undetected intruder and a traffic conflict			W	S	S			
HC3	Radar degradation, leading to undetected intruder and a traffic conflict			W	S				
HC5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and a traffic conflict			W	W	S	W		
HC6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to a traffic conflict			W		S			
HC8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a traffic conflict			W	S	S	S		
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict			W	S	S	S		
HN6	Loss of aircraft power due to engine failure that results in an off field landing, resulting in aircraft damage							S	
HN7	Loss of aircraft power due to electrical failure that results in an off field landing, resulting in aircraft damage							S	
HN8	Catastrophic aircraft system failure that results in a crash and ground fatalities							S	
HN9	Loss of datalink that results in a near-mid-air-collision (NMAC)			W				S	
HN13	Loss of datalink that results in a traffic conflict.			W				S	

Step 6

Repeat the step of accessing across the rows at only those hazards the pilot, sensor operator, and all other traffic influence and determine what other system element influences the majority of those hazards identified. In this situation it is a tie between the

radar and radar data processing unit. This is consistent with reality because they have similar functions in the sensing function of the GBSAA system. Now, continue to repeat steps 5 and 6 until the systems elements and hazards no longer need to be adjusted.

With only a few system elements left, the attention of the builder should focus on the hazards and system elements that have not already been arranged. For the example, it only leaves a few rows and columns located at the bottom right-hand side of the matrix. The process of moving the most similar influences to the left and upward to join the cluster should take place, if possible.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HC3	Radar degradation, leading to undetected intruder and a traffic conflict			W	S				
HC5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and a traffic conflict			W	W	S	W		
HC6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to a traffic conflict			W		S			
HC8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a traffic conflict			W	S	S	S		
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict			W	S	S	S		
HN9	Loss of datalink that results in a near-mid-air-collision (NMAC)			W				S	
HN13	Loss of datalink that results in a traffic conflict.			W				S	
HN6	Loss of aircraft power due to engine failure that results in an off field landing, resulting in aircraft damage							S	
HN7	Loss of aircraft power due to electrical failure that results in an off field landing, resulting in aircraft damage							S	
HN8	Catastrophic aircraft system failure that results in a crash and ground fatalities							S	

Step 9

Once the rearranging is complete, cluster identification begins.

The clusters are identified by a cluster of hazards that are influenced by system elements. With that description, the visual form of clusters is groups of hazards in rows with the system element influences shown in each column. Starting with the upper left corner of the matrix the first cluster can be identified. For the example, the single influence is a single cluster of 1 x 1 (rows x columns) dimension. This cluster only contains one hazard that is influenced by one system element. This satisfies the goal to create a cluster with no interaction with other clusters and it contains no empty boxes.

		System Elements							
No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S	W						
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S	W						
HN4	Crew loses situational awareness of RPA status, leading to NMAC	S	S	W					
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict	S	S	W					
	Pilot commands unsafe maneuver that results	S	S	W					

Cluster 1 Colored Blue

Moving downward from the first cluster, the next influence cluster is identified as a 2 x 2 cluster where only two systems and two hazards influence each other. This cluster contains two hazards that are influenced by the same two system elements. No empty boxes are contained within the cluster.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S	W						
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S	W						
	Crew loses situational awareness of RPA status,	S	S	W					

Cluster 2 Colored Green

Next, below cluster 2 is the next influence cluster identified as a 5 x 3 cluster where only five hazards are influenced by the same three system elements, and no empty boxes are contained within the cluster.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HN1	Pilot-induced oscillation (PIO) that results in aircraft crashing	S							
HN2	Pilot executing improper take-off or landing procedures that results in aircraft departing runway	S	W						
HN3	Loss of aircraft control (on the ground) due to procedural error. Could result in ground fatalities.	S	W						
HN4	Crew loses situational awareness of RPA status, leading to NMAC	S	S	W					
HN5	Crew loses situational awareness of RPA status, leading to a traffic conflict	S	S	W					
HN12	Pilot commands unsafe maneuver that results in a NMAC	S	S	W					
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W	S	W					
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W	S	W					
	RPA is not able to maneuver in time to avoid a	W		W				S	

Cluster 3 Colored Yellow

Below cluster 3 is the next influence cluster is identified as a cluster where four hazards are influenced by the same system five elements. There is no interaction with other clusters. The empty boxes contained within the cluster are discussed in Section 6.3. The four hazards are clustered by visual inspection. The empty boxes between the five system elements are an artifact of the extension of the cluster to include the elements of

RPA and ATC and are shaded a light red color. Those empty boxes are not considered a part of the cluster. The extension of including the RPA and ATC system elements in the cluster creates a different cluster of hazards from cluster 3.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HC4	Intruder is not noticed by RPA crew, leading to a traffic conflict	W	S	W					
HA4	Intruder is not noticed by RPA crew, leading to failure to respond to intruder and NMAC	W	S	W					
HA11	RPA is not able to maneuver in time to avoid a potential NMAC	W		W				S	
HC10	Inability to communicate with ATC, resulting in traffic conflict	S	S	W					S
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities	S	W					W	S
HN11	Uncommanded altitude or course deviation that results in a NMAC	S	W	W				S	S
	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly	S	W	W	W	S	W		

Cluster 4 Colored Maroon

The next cluster of hazards contains a group of three hazards that are the only influenced by the same set of six system elements. There is no interaction with other clusters and no empty boxes are contained within the cluster.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HN10	Failure to avoid hazardous weather resulting in loss of aircraft and/or ground fatalities	S	W					W	S
HN11	Uncommanded altitude or course deviation that results in a NMAC	S	W	W				S	S
HA7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to NMAC	S	W	W	W	S	W		
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	W	S	S	W		
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	S	W	W	W	S	W		
	Airspace display failure, leading to undetected		W	W	W	W	S		

Cluster 5 Colored Red

Below cluster 5, a pair of hazards contains are only influenced by the same set of five system elements. These five system elements are similar to those elements in cluster 5, but this separate cluster satisfies the primary goals of the clustering. There is no interaction with other clusters and no empty boxes are contained within the cluster.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HA10	Erroneous data leads pilot to command unsafe maneuver, resulting in NMAC	S	S	W	S	S	W		
HC7	Pop-up intruder inside Threat Volume with insufficient time to react, with a properly functioning system, leading to a traffic conflict	S	W	W	W	S	W		
HA1	Airspace display failure, leading to undetected intruder and NMAC		W	W	W	W	S		
HC1	Airspace display failure, leading to a traffic conflict		W	W	W	W	S		
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC			W	S	S			
HA3	Radar degradation, leading to undetected intruder and NMAC			W	S				
	Detection and tracking software failure,			W	W	S	W		

Cluster 6 Colored Dark Orange

Moving downward from cluster 6, the next set of clustered hazards are influenced by the same set of four system elements. This cluster contains twelve hazards. There is no interaction with other clusters and only a few empty boxes.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HC1	Airspace display failure, leading to a traffic conflict		W	W	W	W	S		
HA2	Communication failure between radar and radar data processing unit, leading to undetected intruder and NMAC			W	S	S			
HA3	Radar degradation, leading to undetected intruder and NMAC			W	S				
HA5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and NMAC			W	W	S	W		
HA6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to NMAC			W	W	S			
HA8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a NMAC			W	S	S	S		
HA9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and NMAC			W	S	S	S		
HC2	Communication failure between radar and radar data processing unit, leading to undetected intruder and a traffic conflict			W	S	S			
HC3	Radar degradation, leading to undetected intruder and a traffic conflict			W	S				
HC5	Detection and tracking software failure, leading to incomplete intruder information (includes failure to alert, etc.) and a traffic conflict			W	W	S	W		
HC6	Untracked intruder inside Threat Volume, with a properly functioning system, leading to a traffic conflict			W	W	S			
HC8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a traffic conflict			W	S	S	S		
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict			W	S	S	S		
	Loss of datalink that results in a near-mid-air-			W				S	

Cluster 7 Colored Light Orange

After cluster 7, a pair of hazards contains are only influenced by the same set of two system elements. Even though there are visible empty boxes between the two systems, this is still considered a 2 x 2 cluster due to two hazards and two elements. The space between the elements is an artifact of the cluster technique as it approached the end of the matrix. There is no interaction with other clusters and no empty boxes are contained within the cluster.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict			W	S	S	S		
HN9	Loss of datalink that results in a near-mid-air-collision (NMAC)			W				S	
HN13	Loss of datalink that results in a traffic conflict.			W				S	
	Loss of aircraft power due to engine failure that results in an off field landing, resulting in							S	

Cluster 8 Colored Green

With all other clusters indentified, only a group of three hazards remained that are only influenced by the same system element. There is no interaction with other clusters and no empty boxes are contained within the cluster.

No.	Hazard	Pilot	Sensor Operator	All Other Air Traffic	Radar(s)	Radar Data Processing Unit	Airspace Display	RPA	Air Traffic Controller	
HC8	Limited sense and avoid capability (GBSAA drop out during mission), resulting in a traffic conflict			W	S	S	S			
HC9	Degraded GBSAA system (due to weather, etc.) leads to undetected intruder and traffic conflict			W	S	S	S			
HN9	Loss of datalink that results in a near-mid-air-collision (NMAC)			W				S		
HN13	Loss of datalink that results in a traffic conflict.			W				S		
HN6	Loss of aircraft power due to engine failure that results in an off field landing, resulting in aircraft damage							S		
HN7	Loss of aircraft power due to electrical failure that results in an off field landing, resulting in aircraft damage							S		
HN8	Catastrophic aircraft system failure that results in a crash and ground fatalities							S		

Cluster 9 Colored Blue

(this page intentionally left blank)

Bibliography

1. United States. Federal Aviation Administration. Aviation Safety Unmanned Aircraft Program Office. Interim Operational Approval Guidance 08-01, Unmanned Aircraft Systems Operations in the U. S. National Airspace System. FAA, 2008. Print.

2. United States. Air Force Safety Center. Unmanned Aerial Systems. Risk Management for Flying Predator in the National Airspace at Cannon, NM. Kirtland AFB, 2012. Print.

3. United States. Federal Aviation Administration. System Safety Handbook. 30 December 2000.

4. United States. Department of Defense. Office of the Secretary of Defense. FY2009-2034 Unmanned Systems Integrated Roadmap. DoD, 2009. Print.

5. "Policy Options for Unmanned Aircraft Systems." Congressional Budget Office, 2011. PDF. 13 Dec. 2011.

6. United States. Department of Defense. UAS Task Force Airspace Integration Integrated Product Team. Unmanned Aircraft System Airspace Integration Plan. Version 2.0. DoD, 2011. Print.

7. Wise, Jeff. "Civilian UAVs: No Pilot, No Problem - Popular Mechanics." PopularMechanics.com. Popular Mechanics, 1 Oct. 2009. Web. 13 Dec. 2011. <http://www.popularmechanics.com/science/space/4213464>.

8. "NASA - NASA Dryden Fact Sheet - Altair/Predator B." NASA.gov. NASA, 7 May 2006. Web. 13 Dec. 2011. <http://www.nasa.gov/centers/dryden/news/FactSheets/FS-073-DFRC.html>.

9. Bennett, Brian. "Police Employ Predator Drone Spy Planes on Home Front - Latimes.com." Los Angeles Times - California, National and World News - Latimes.com. Washington Bureau, 10 Dec. 2011. Web. 13 Dec. 2011. <http://www.latimes.com/news/nationworld/nation/la-na-drone-arrest-20111211.0.324348.story>.

10. "Fact Sheet – Unmanned Aircraft Systems (UAS)." FAA: Home. Web. 20 Oct. 2010. <http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=6287>.

11. "FAA Regulations." FAA: Home. Web. 20 Oct. 2011. http://www.faa.gov/regulations_policies/faa_regulations/

12. "Unmanned Aircraft System (UAS) Sense and Avoid (SAA) Technology Development Roadmap." Office of Security Review Department of Defense (2010). Print.

13. United States. Federal Aviation Administration. Order 7610.4. Special Operations. 2001.

14. "DOT Organizations." U.S. Department of Transportation. US DOT, 27 May 2009. Web. 26 Oct. 2011. <http://www.dot.gov/summary.htm>.

15. "Aeronautical Information Manual." FAA.gov. Federal Aviation Administration, 11 Feb. 2010. Web. 13 Dec. 2011. <http://www.faa.gov/air_traffic/publications/atpubs/aim/index.htm>.

16. Nolan, Michael S. Fundamentals of Air Traffic Control. 4th ed. Belmont, CA: Brooks/Cole, Cengage Learning, 2004. Print.

17. Weibel, Roland E. Safety Considerations for Operation of Different Classes of Unmanned Aerial Vehicles in the National Airspace System. Thesis. Massachusetts Institute of Technology, 2005. Cambridge, MA: MIT Libraries, 2005. Print.

18. Weibel, Roland E. Assuring Safety through Operational Approval: Challenges in Assessing and Approving the Safety of System-Level Changes in Air Transportation. Thesis. Massachusetts Institute of Technology, 2009. Cambridge, MA: MIT Libraries, 2009. Print.

19. SAE Standards. "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment." Aircraft And Sys Dev And Safety Assessment Committee, ARP 4761, December 1 1996. Web. 25 Oct. 2011. <http://standards.sae.org/arp4761/>.

20. United States. Department of Defense. Military Standard Practice for System Safety. 2005. Print. 882E.

21. Eurocontrol Experimental Centre. European Organisation for the Safety of Air Navigation. Review of Techniques to Support the EATMP Safety Assessment Methodology. Vol. 1. 2004. Print.

22. United States. Federal Aviation Administration, "Safety Management System Manual," Air Traffic Organization. Version 2.1, May 2008

23. IEEE Computer Society. Software Engineering Standards Committee. IEEE Recommended Practice for Architectural Description of Software-Intensive Systems. New York, NY: Institute of Electrical and Electronics Engineers, 2000. Print. Std 1471-2000.

24. "DOD Dictionary of Military and Associated Terms." DTIC Online. Joint Education and Doctrine Division, 8 Nov. 2010. Web. 25 Aug. 2011. <http://www.dtic.mil/doctrine/dod_dictionary/>.

25. Ericson, Clifton A. "Fault Tree Analysis - A History." The 17th International System Safety Conference. Orlando, FL. Aug. 1999. Reading.

26. "Albuquerque Sectional Chart." SkyVector Aeronautical Charts. Flight Prep, 2012. Web. 27 Mar. 2012. <http://skyvector.com/>.

27. "Airport Data & Contact Information." FAA: Home. US Department of Transportation, 5 Apr. 2012. Web. 26 Apr. 2012. <http://www.faa.gov/airports/airport_safety/airportdata_5010/>.

28. United States. Federal Aviation Administration. Certificate of Waiver or Authorization. Cannon Air Force Base Air Traffic Control Tower #2011-CSA-2-MOA, 7 June 2011. Print.

29. Francis, Roger. "Gray Butte & Cannon Ground Based Sense and Avoid Demonstrations." CNS/ATM Conference. 2011. AFCEA Boston. The MITRE Corporation, 2011. Web. 29 Feb. 2012. <www.afceaboston.com>.

30. "Launch and Recovery GCS." General Atomics Aeronautical. General Atomics, 2012. Web. 27 Jan. 2012. <http://www.ga-asi.com/products/ground_control/launch_recovery.php>.

31. "MQ-1B PREDATOR Factsheet." AF.mil. U.S. Air Force, 20 July 2010. Web. 13 Dec. 2011. <http://www.af.mil/information/factsheets/factsheet.asp?fsID=122>.

32. Valerdi, Ricardo, Nenad Medvidovic, George Edwards, C. Robert Kenley, and Filiberto Macias. "Identification and Prioritization of High-Value Test Scenarios for Autonomous Systems via Architectural Analysis." MIT (2010). Print.

33. Yu, Tian-Li, David E. Goldberg, Kumara Sastry, and Claudio F. Lima. "Dependency Structure Matrix, Genetic Algorithms, and Effective Recombination." Evolutionary Computation 17.4 (2009): 595-626. Print.

34. Black, Thomas A., Charles H. Fine, and Emanuel M. Sachs. "A Method for Systems Design Using Precedence Relationships: An Application to Automotive Brake Systems." MIT ESD Working Paper Series 3208-90 (1990). Print.

35. Browning, Tyson R. "Applying the Design Structure Matrix to System Decomposition and Integration Problems: A Review and New Directions." IEEE Transactions on Engineering Management 48.3 (2001): 292-306. Print.

36. Browning, Tyson R. "The Design Structure Matrix." Technology Management Handbook (2000): 103-11. Print.

37. Gulati, Rosaline K., and Steven D. Eppinger. "The Coupling of Product Architecture and Organizational Structure Decisions." MIT Sloan School of Management Working Paper 3906 (1996). Print.

38. Gulati, Rosaline K. The Coupling of Product Architecture and Organizational Sturcture Decisions. Thesis. Massachusetts Institue of Technology, 1996. Cambridge: MIT Libraries, 1996. Print.

39. Pimmler, Thomas U., and Steven D. Eppinger. "Integration Analysis of Product Decompositions." ASME Design Theory and Methodology Conference. Minneapolis, MN. Sept. 1994.

40. Sharon, Amira, Dov Dori, and Olivier De Weck. "Model-Based Design Structure Matrix: Deriving a DSM from an Object-Process Model." Second International Symposium on Engineering Systems. Massachusetts Institute of Technology, Cambridge, MA. 15 June 2009. Reading.

41. Yassine, Ali A., Daniel E. Whitney, Jerry Lavine, and Tony Zambito. "Do-It-Right-First-Time (DRFT) Approach to DSM Restructuring." MIT ESD Working Paper Series 04 (2001). Print.